Защищённое удалённое место сотрудника.

Общая концепция.

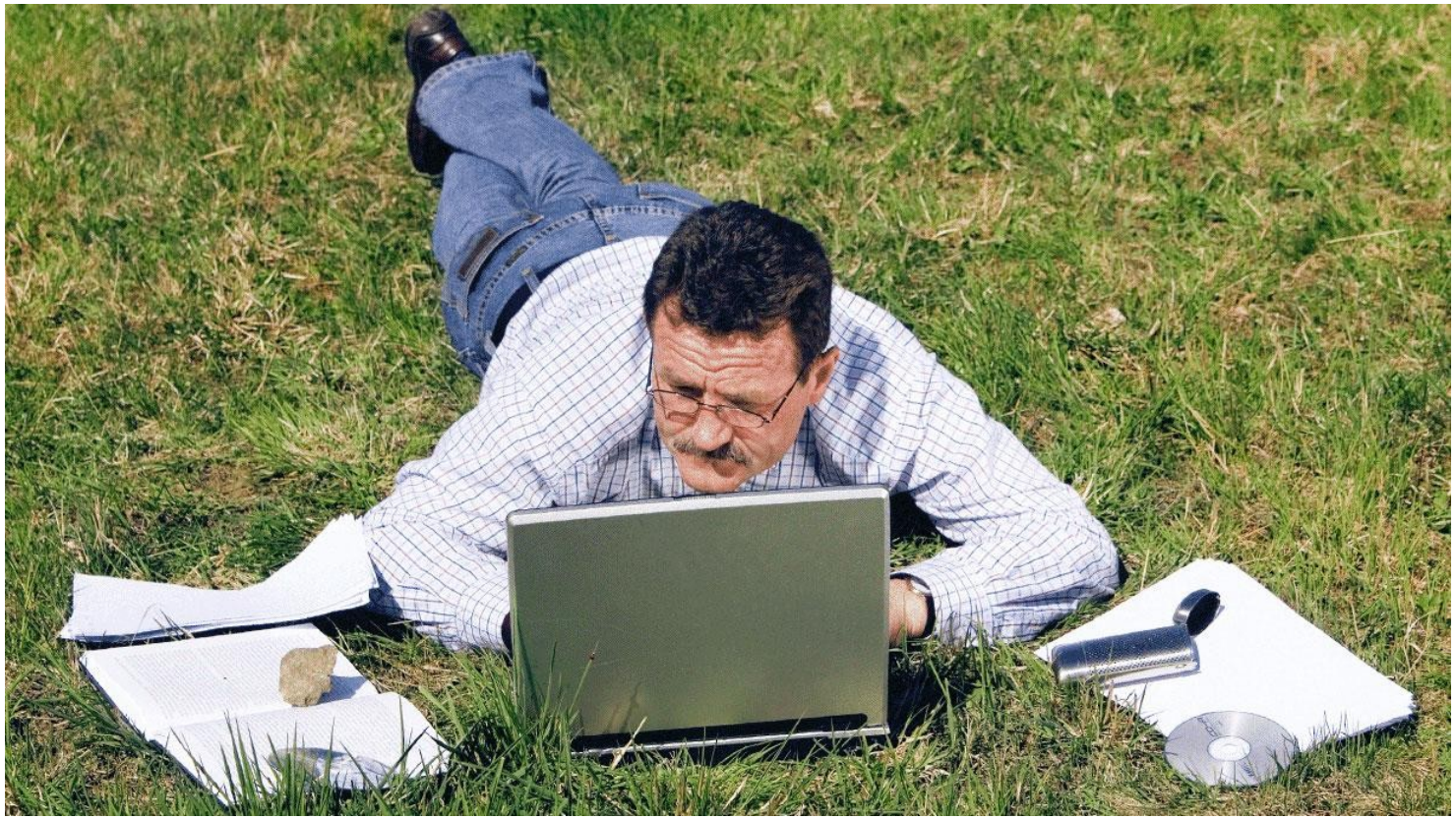
Ведущий инженер-программист
Фадин Сергей Юрьевич

РЕДСОФТ

Москва, 2021

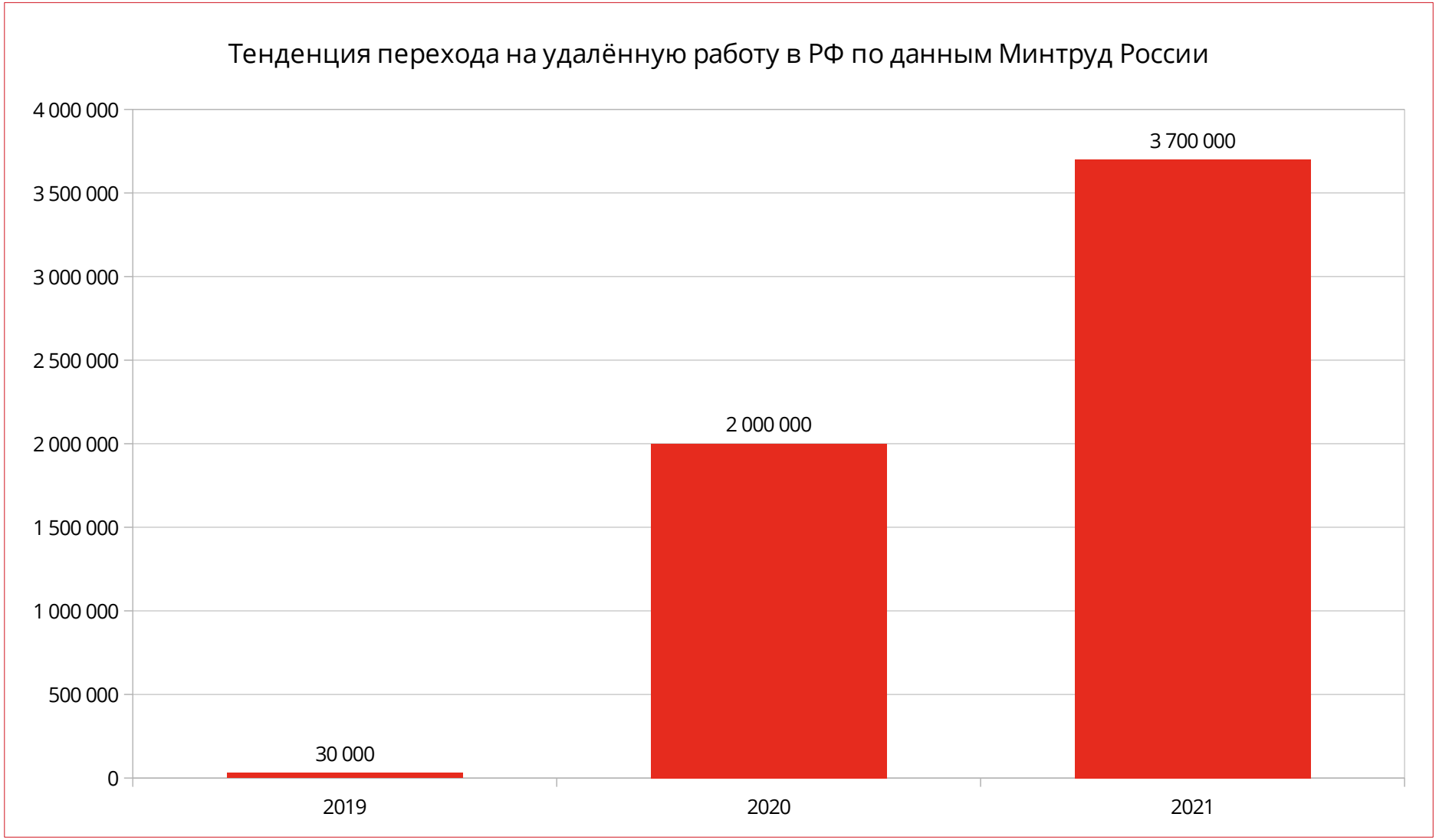
Введение

Удалённая работа — это когда не нужно каждый день ездить в офис, а работать там, где комфортно.



РЕДСОФТ

Статистика перехода на удалённую работу



РЕДСОФТ

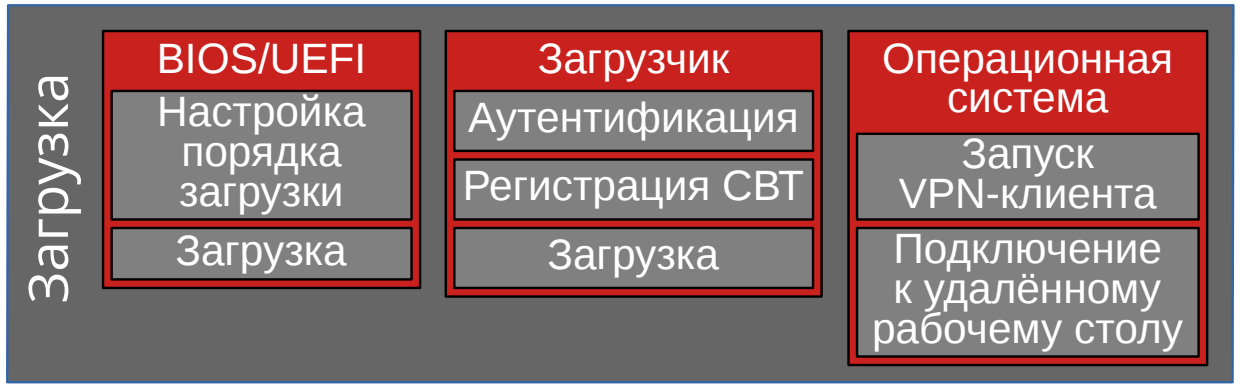
Требования к аппаратной части

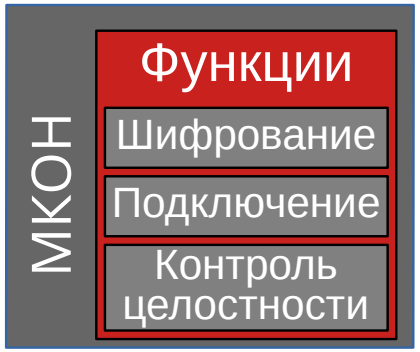
- Загрузчик операционной с проверкой контрольных сумм;
- Возможность привязки к аппаратному обеспечению;
- Защищённое хранилище ключей и паролей;
- Запуск операционной системы и доступ к шифрованным разделам только после предварительной аутентификации на этапе загрузки.

Требования к программной части

- Запуск только с защищённого носителя информации;
- Минимально необходимый для работы набор программного обеспечения;
- Система контроля целостности файлов операционной системы;
- Возможность многофакторной аутентификации входа в систему;
- Невозможность использование расширенных привилегий пользователя, а так же запуска приложений не из списка разрешённых;
- Сохранять данные подключения к сети, регистрацию программного обеспечения и иметь возможность изменять эти данные средствами операционной системы и системы администрирования;
- Автоматически и мгновенно завершать работу системы при извлечении носителя информации, который содержит записанный образ операционной системы.

Структура изделия





РЕДСОФТ

Описание разделов изделия

Загрузочный раздел	LiveBoot на базе ядра Linux, который реализует следующие функции: Контроль целостности образа ОС Аутентификация и авторизация перед загрузкой операционной системы Регистрация СВТ
Системный раздел	Образ сертифицированной ОС «РЕД ОС» с интегрированным ПО
Защищённый прикладной раздел	Реквизиты, необходимые для подключения к VPN Раздел может содержать реквизиты, необходимые для подключения к «удаленному рабочему столу»
Защищённый раздел данных	В раздел сохраняется экземпляр директории /home пользователя, данные сетевых подключений. Выполняется хранение результатов сеанса работы операционной системы. На дисковом устройстве хранятся данные отдельного раздела (логического диска) «Данных пользователя»
Раздел информации	Информационные материалы: ▪ «Инструкции и руководства» ▪ «Видео инструкции»
Служебный раздел	Журналы событий: ▪ «Журнал Событий ОС» ▪ «Журнал Событий Безопасности» ▪ Контрольные суммы

Инструменты реализации

- **РЕД ОС** — операционная система на базе ядра Linux;
- **Pungi** — инструмент для создания дистрибутива, который отслеживает правильность запускаемых скрипов в требуемом порядке и необходимыми аргументами;
- **Lorax** — инструмент формирования загрузочного образа операционной системы;
- **QEMU** — эмулятор аппаратного обеспечения различных платформ;
- **JaCarta** — USB-токены, смарт-карты и модули безопасности для аутентификации, формирования и проверки электронной подписи, шифрования передаваемых данных, а также безопасного хранения объектов и информации пользователя;
- **SecureAdmin** — инструмент записи образа ОС на USB-токен JaCarta.

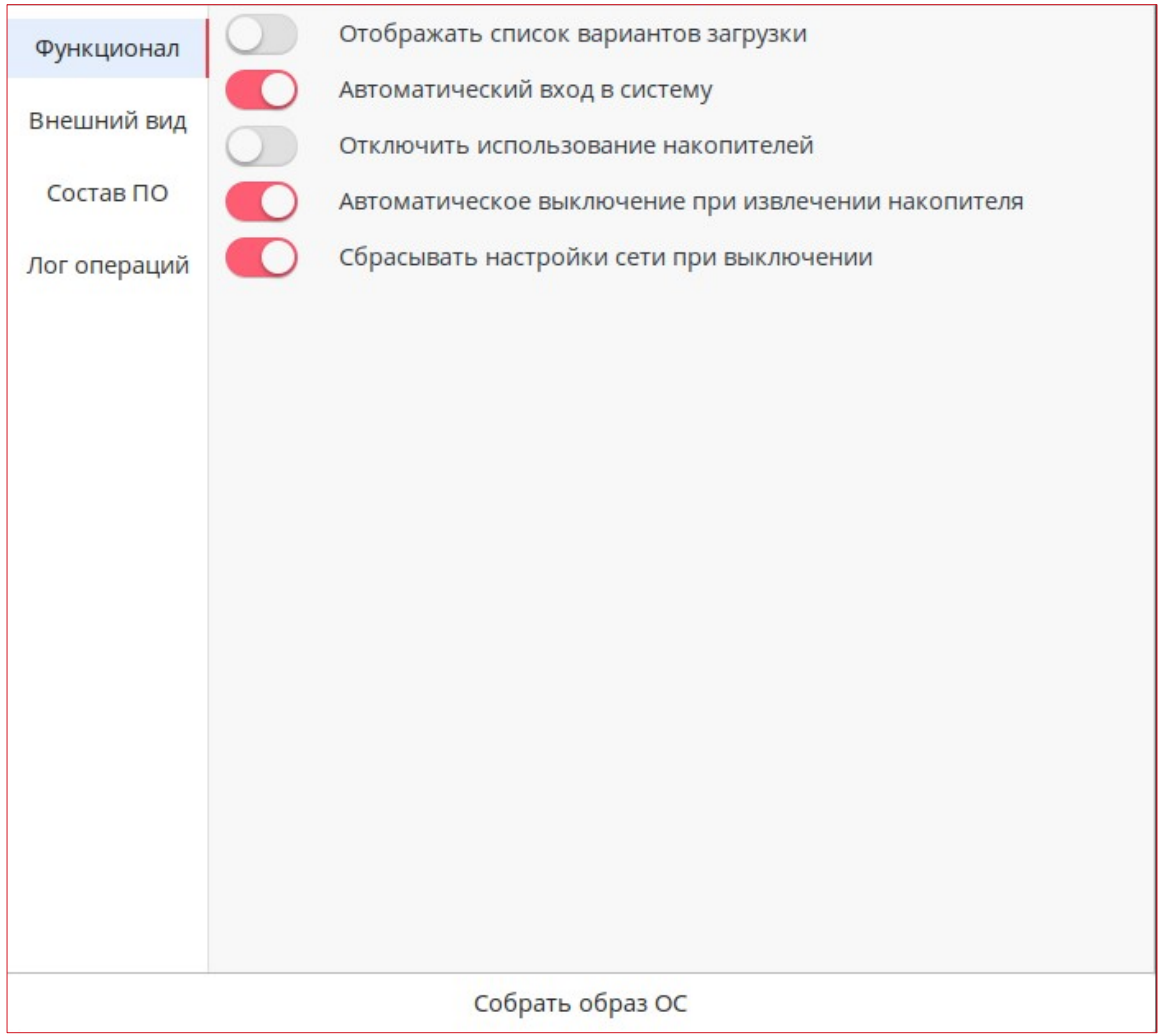
Проблемы и решения

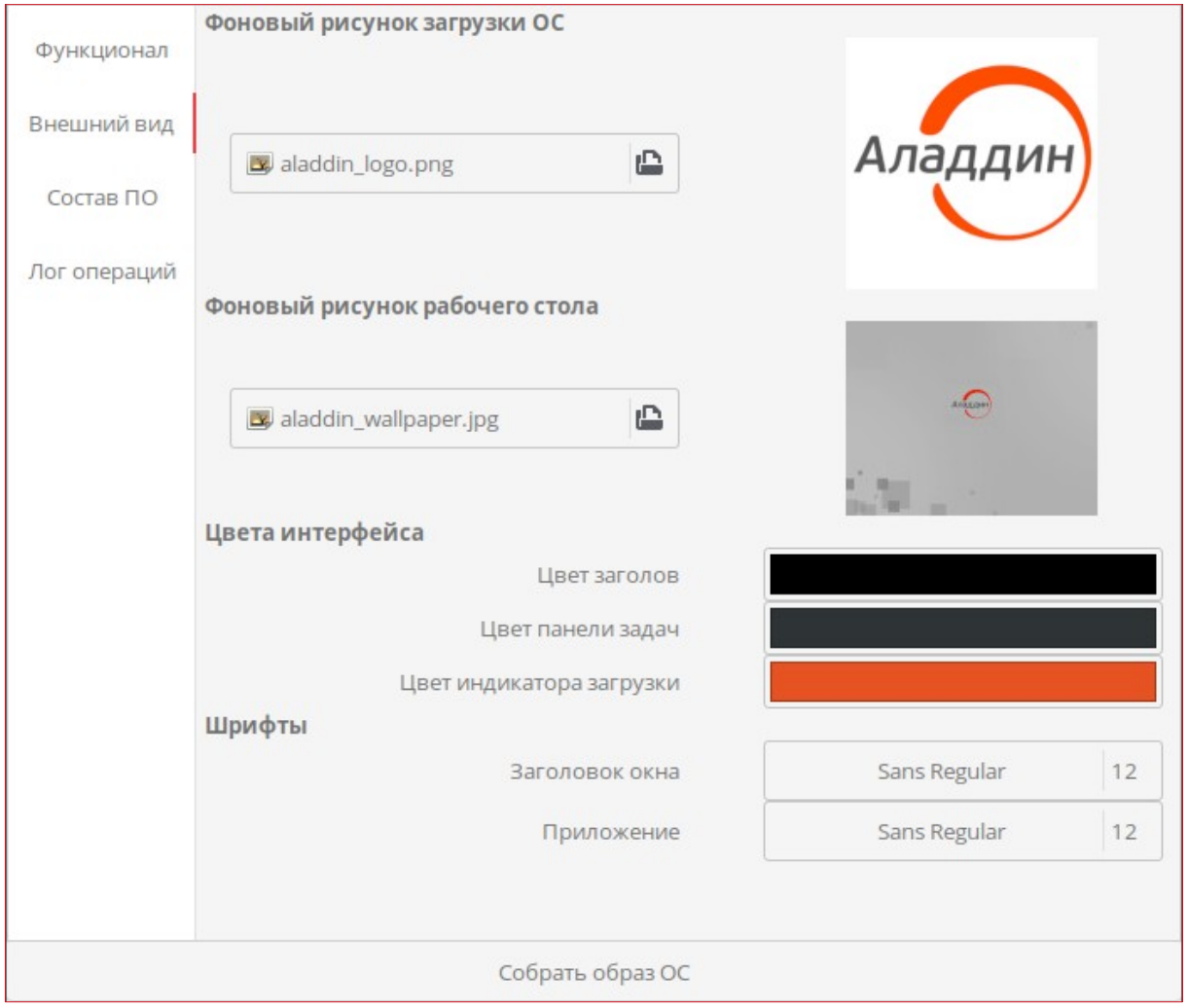
Проблема	Решение
Отсутствие конкретных требований к системе удалённого рабочего места сотрудника с использование защищённого программно-аппаратного комплекса.	Исследование потребностей рынка. Создание и тестирование прототипов системы различной направленности.
Выбор защищённого носителя информации.	Компания «Аладдин Р.Д.» предоставила защищённый носитель информации «JaCarta» и специальную прошивку под реализацию проекта.
Выбор защищённого носителя информации.	Компания «Аладдин Р.Д.» предоставила защищённый носитель информации «JaCarta» и специальную прошивку под реализацию проекта.
Трудоёмкая подготовка и внесение одинаковых изменений в образы ОС с различным составом ПО.	Автоматизировать сборку образов ОС с использованием сценариев интеграции различного ПО, а так же обозначить все несовместимые сценарии использования и заранее обезопасить себя и конечного потребителя от вероятных проблем совместимости.

Состав конструктора ОС

- Набор скриптов
- Интерфейс отладки
- Гибкий конфигуратор
- Разрешение конфликтов ПО
- Пользовательский GUI

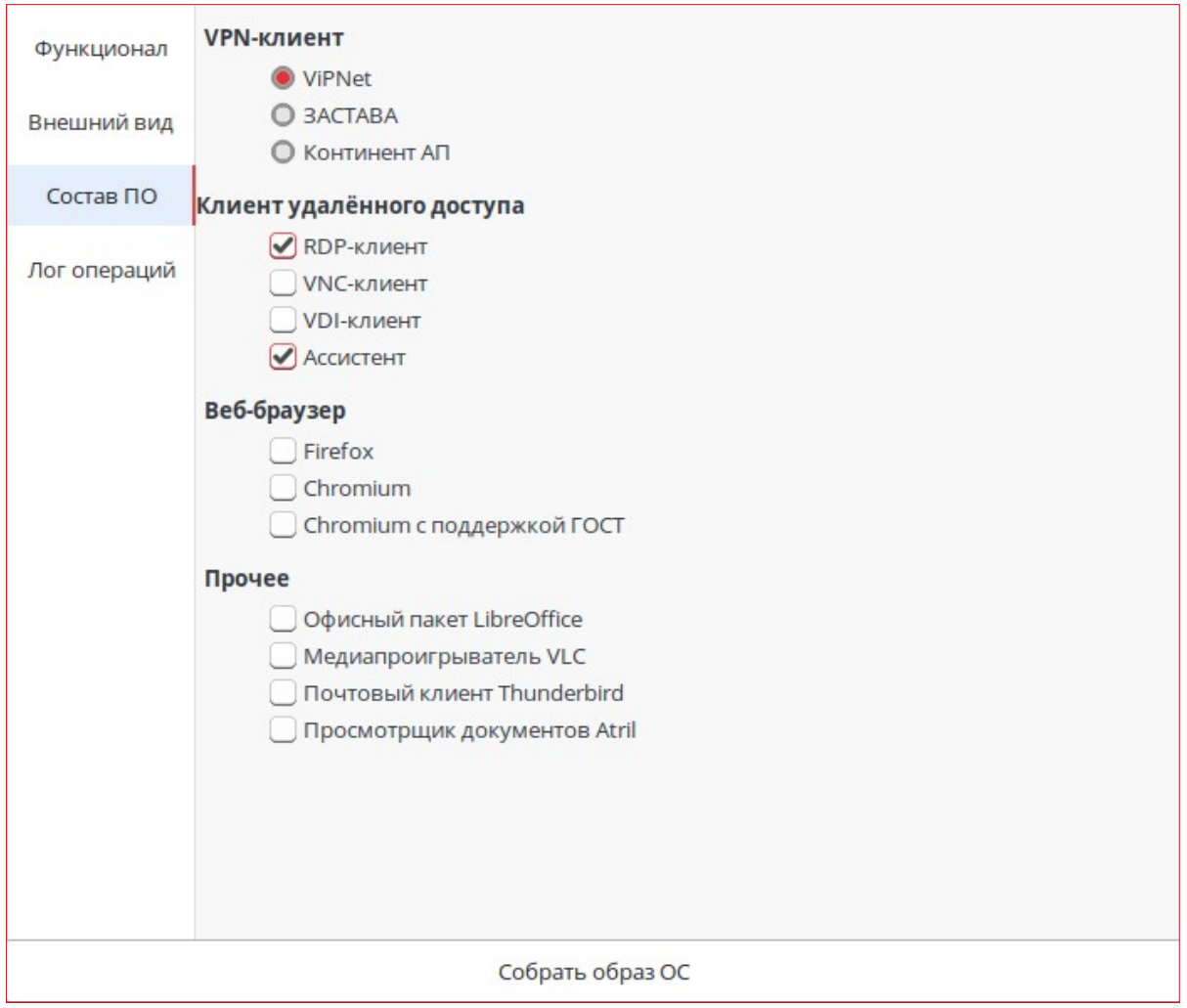
GUI конструктора ОС

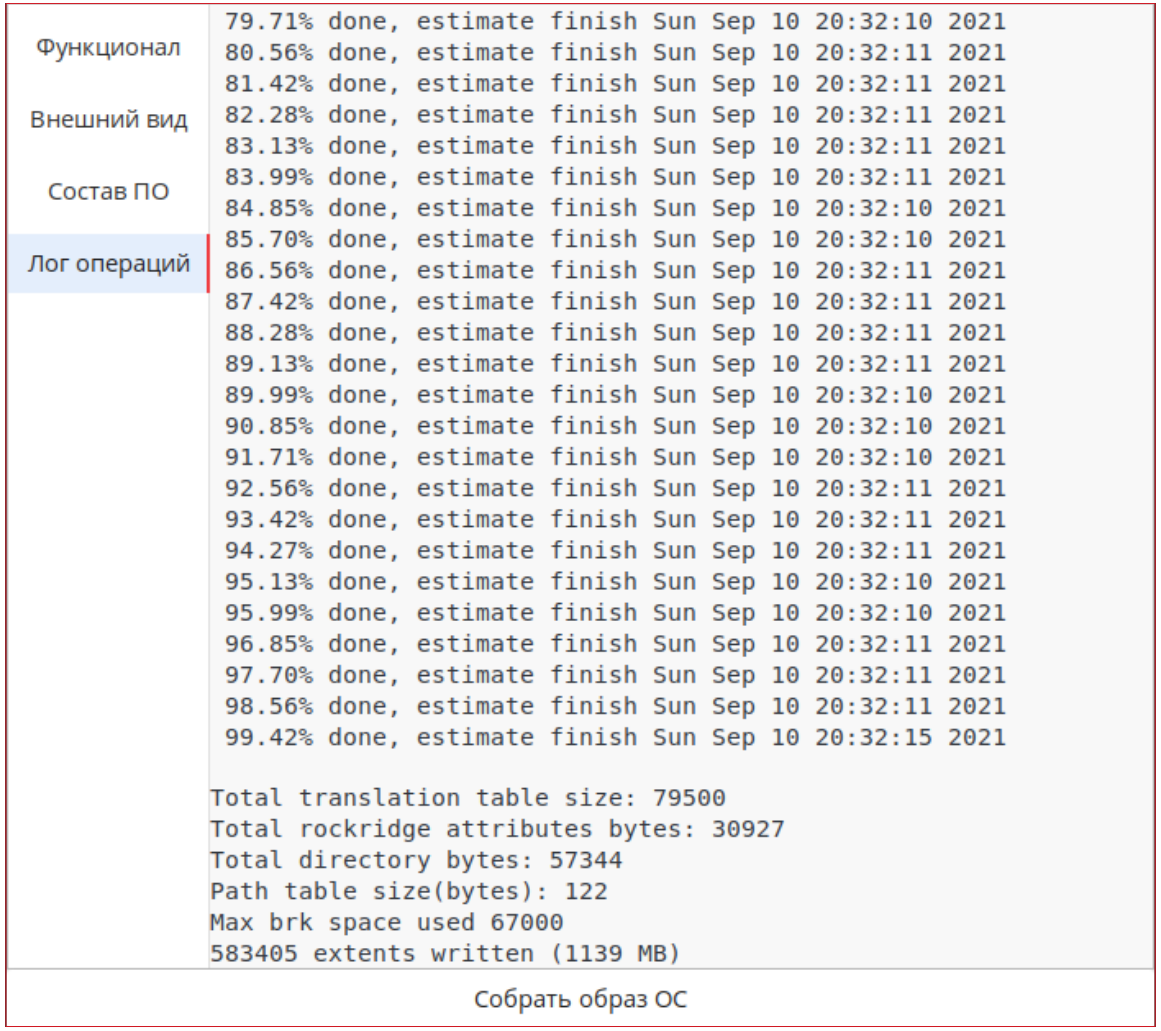




РЕДСОФТ

GUI конструктора ОС





РЕДСОФТ

Пример результата работы конструктора ОС

Планы развития конструктора ОС

- Добавить выбор типа рабочего окружения;
- Расширить совместимость с ПО сторонних разработчиков;
- Перенести конструктор на веб-версию;
- Интегрировать конструктор со средой тестирования «Tooster»;
- Реализовать возможность обновления ранее сформированных сборок ОС;
- Отказаться от использования пакетного менеджера для исключения ненужных зависимостей и сокращения объёма образа ОС;
- Рассмотреть возможность сборки специализированного ядра ОС.

Итоги

«Между работой из дома и работой в офисе возникает здоровая конкуренция, которая идёт на пользу всем. Офисы становятся более домашними, а специалисты — более дисциплинированными. Появляются новые средства для коллективной работы. Мы тратим меньше бумаги, но при этом производим больше контента.»

Александр Мезин

БЛАГОДАРИМ ЗА ВНИМАНИЕ !

www.red-soft.ru