

Защищённое удалённое место сотрудника. Общая концепция.

Ведущий инженер-программист
Федин Сергей Юрьевич



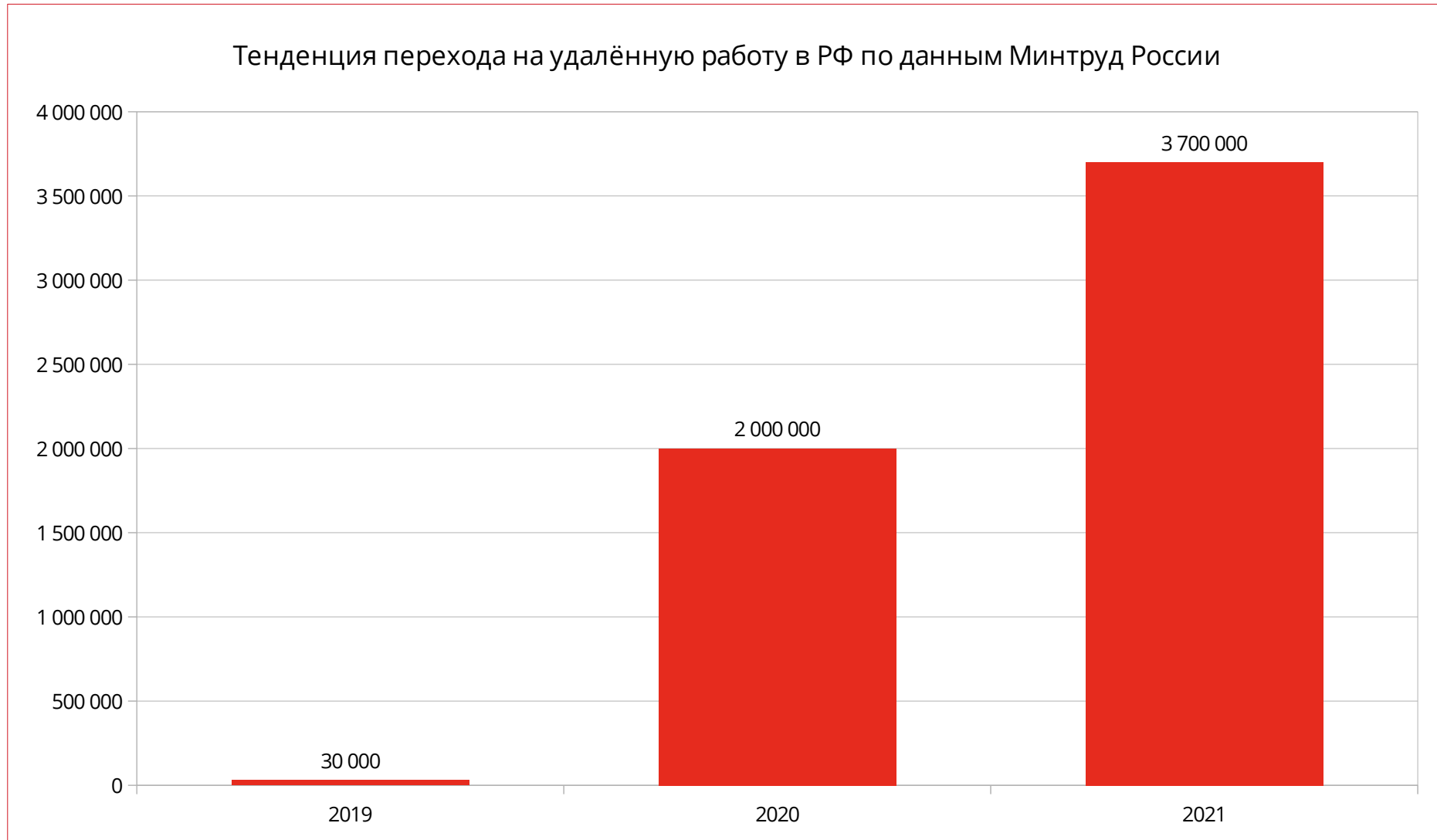
Москва, 2021

Введение

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



Статистика перехода на удалённую работу



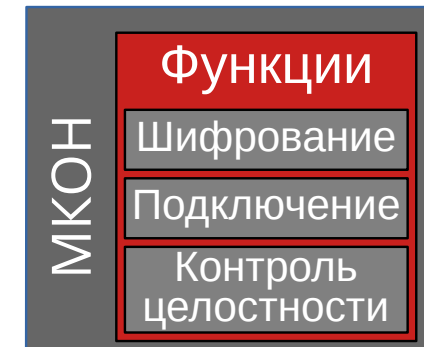
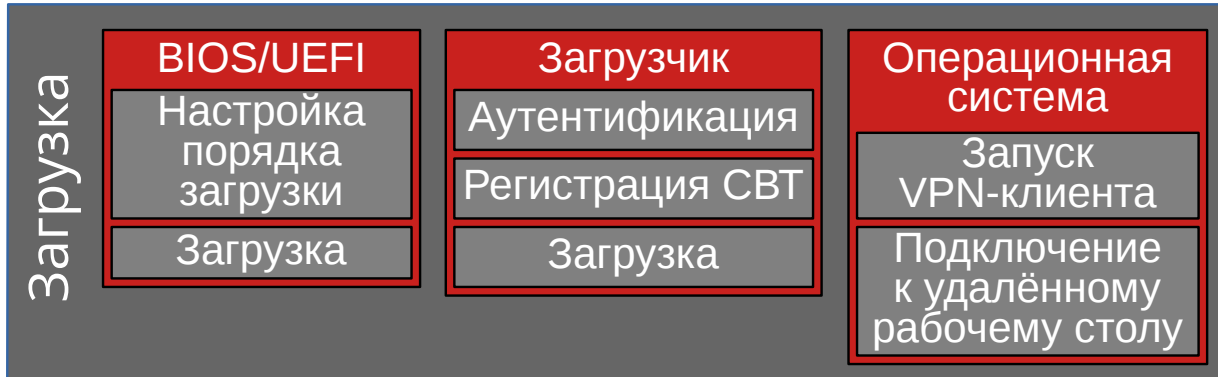
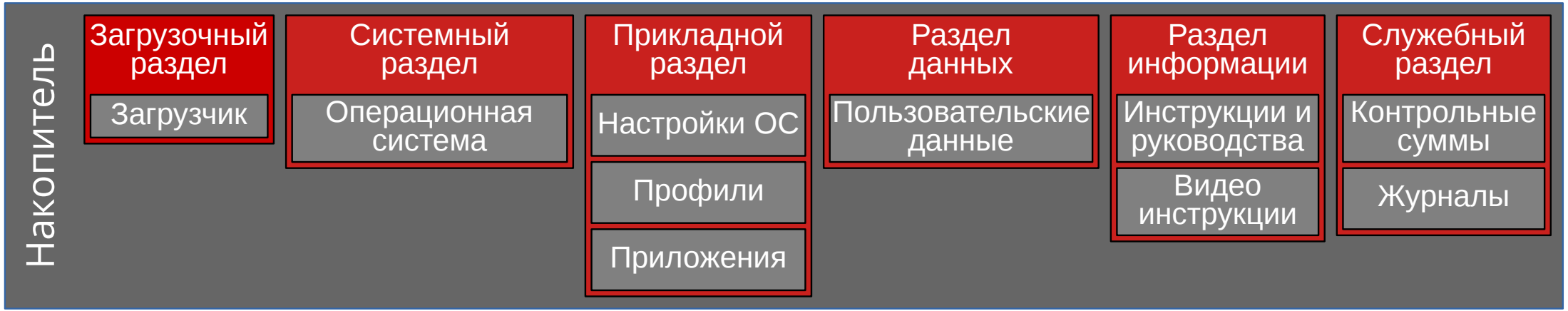
Требования к аппаратной части

- Загрузчик операционной с проверкой контрольных сумм;
- Возможность привязки к аппаратному обеспечению;
- Защищённое хранилище ключей и паролей;
- Запуск операционной системы и доступ к зашифрованным 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



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: <ul style="list-style-type: none">▪ «Инструкции и руководства»▪ «Видео инструкции»
Служебный раздел	Журналы событий: <ul style="list-style-type: none">▪ «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 скриптов 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 использованием 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

Функционал	<input type="checkbox"/>	Отображать список вариантов загрузки
Внешний вид	<input checked="" type="checkbox"/>	Автоматический вход в систему
Состав ПО	<input type="checkbox"/>	Отключить использование накопителей
Лог операций	<input checked="" type="checkbox"/>	Автоматическое выключение при извлечении накопителя
	<input checked="" type="checkbox"/>	Сбрасывать настройки сети при выключении

Собрать образ ОС

Функционал	Фоновый рисунок загрузки ОС	
Внешний вид	<input type="text" value="aladdin_logo.png"/>	
Состав ПО	Фоновый рисунок рабочего стола	
Лог операций	<input type="text" value="aladdin_wallpaper.jpg"/>	
	Цвета интерфейса	
	Цвет заголов	<input type="text" value="black"/>
	Цвет панели задач	<input type="text" value="darkgray"/>
	Цвет индикатора загрузки	<input type="text" value="orange"/>
	Шрифты	
	Заголовок окна	<input type="text" value="Sans Regular"/> 12
	Приложение	<input type="text" value="Sans Regular"/> 12

Собрать образ ОС

GUI конструктора ОС

Функционал	VPN-клиент
Внешний вид	<input checked="" type="radio"/> ViPNet <input type="radio"/> ЗАСТАВА <input type="radio"/> Континент АП
Состав ПО	Клиент удалённого доступа
Лог операций	<input checked="" type="checkbox"/> RDP-клиент <input type="checkbox"/> VNC-клиент <input type="checkbox"/> VDI-клиент <input checked="" type="checkbox"/> Ассистент
	Веб-браузер
	<input type="checkbox"/> Firefox <input type="checkbox"/> Chromium <input type="checkbox"/> Chromium с поддержкой ГОСТ
	Прочее
	<input type="checkbox"/> Офисный пакет LibreOffice <input type="checkbox"/> Медиапроигрыватель VLC <input type="checkbox"/> Почтовый клиент Thunderbird <input type="checkbox"/> Просмотрщик документов Atril
Собрать образ ОС	

Функционал	79.71% done, estimate finish Sun Sep 10 20:32:10 2021
Внешний вид	80.56% done, estimate finish Sun Sep 10 20:32:11 2021 81.42% done, estimate finish Sun Sep 10 20:32:11 2021 82.28% done, estimate finish Sun Sep 10 20:32:11 2021
Состав ПО	83.13% done, estimate finish Sun Sep 10 20:32:11 2021 83.99% done, estimate finish Sun Sep 10 20:32:11 2021 84.85% done, estimate finish Sun Sep 10 20:32:10 2021
Лог операций	85.70% done, estimate finish Sun Sep 10 20:32:10 2021 86.56% done, estimate finish Sun Sep 10 20:32:11 2021 87.42% done, estimate finish Sun Sep 10 20:32:11 2021 88.28% done, estimate finish Sun Sep 10 20:32:11 2021 89.13% done, estimate finish Sun Sep 10 20:32:11 2021 89.99% done, estimate finish Sun Sep 10 20:32:10 2021 90.85% done, estimate finish Sun Sep 10 20:32:10 2021 91.71% done, estimate finish Sun Sep 10 20:32:10 2021 92.56% done, estimate finish Sun Sep 10 20:32:11 2021 93.42% done, estimate finish Sun Sep 10 20:32:11 2021 94.27% done, estimate finish Sun Sep 10 20:32:11 2021 95.13% done, estimate finish Sun Sep 10 20:32:10 2021 95.99% done, estimate finish Sun Sep 10 20:32:10 2021 96.85% done, estimate finish Sun Sep 10 20:32:11 2021 97.70% done, estimate finish Sun Sep 10 20:32:11 2021 98.56% done, estimate finish Sun Sep 10 20:32:11 2021 99.42% done, estimate finish Sun Sep 10 20:32:15 2021
Total translation table size: 79500 Total rockridge attributes bytes: 30927 Total directory bytes: 57344 Path table size(bytes): 122 Max brk space used 67000 583405 extents written (1139 MB)	
Собрать образ ОС	

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 «Тоoster»;
- 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.

«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