Безопасное удаленное рабочее место

Работая в офисе, сотрудники используют корпоративные компьютеры и программы, проверенные антивирусом. Подключиться к сети и серверам предприятия можно только из офиса, доступ в который защищен пропусками, охраной и бдительными коллегами.

Но при удаленной работе существует целый ряд угроз: передаваемые по публичным каналам данные могут быть перехвачены или изменены. В случае кражи пароля злоумышленник может подключаться к серверам организации под правами легального пользователя. А если домашний компьютер заражен вирусами, то они смогут попасть на компьютеры предприятия.

Решение для безопасной удаленной работы на базе Рутокен ЭЦП 2.0 Flash позволит:

- Безопасно работать на любом компьютере
- Использовать VPN для взаимодействия с сетью организации
- Хранить информацию на защищенном PIN-кодом разделе
- Реализовать строгую двухфакторную аутентификацию
- Подписывать электронные документы, в том числе с помощью УКЭП
- Использовать одно устройство для всех задач

Состав решения

1 Устройство Рутокен ЭЦП 2.0 Flash

- Объединяет в себе СКЗИ Рутокен ЭЦП 2.0 и защищенный Flash-диск.
- Содержит:
  - разделы для загрузки операционной системы и хранения файлов пользователей;
  - защищенное хранилище ключей и сертификатов;
  - специализированный процессор для выполнения криптографических операций.
- Позволяет:
  - устанавливать права на разделы Flash-памяти;
  - блокировать доступ к разделам Flash-памяти и хранилищу ключей до ввода PIN-кода;
  - вычислять электронную подпись с помощью алгоритмов ГОСТ и RSA;
  - выполнять двухфакторную аутентификацию, как для ОС, так и для клиентов VPN, RDP и т. п.
- Имеет сертификаты ФСТЭК и ФСБ России и совместим с широким спектром программного и аппаратного обеспечения.

2 Операционная система по выбору заказчика

alt linux · ASTRALINUX® · РЕДОС · ROSA · Microsoft

3 Дополнительное программное обеспечение, необходимое конкретному заказчику:

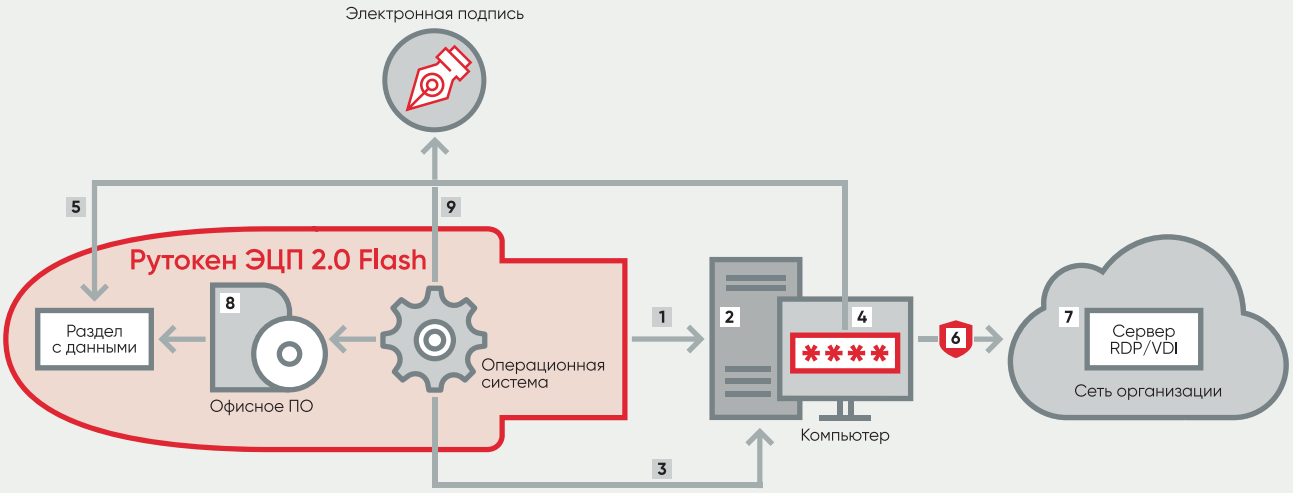
- Клиент RDP/VDI для подключения к удаленным рабочим столам
- Офисное ПО для работы с документами
- Специализированное ПО, необходимое для нужд конкретной организации

4 Клиент VPN для безопасного подключения к сети предприятия

В состав решения может быть включен клиент VPN, используемый в организации:

- NGate (КриптоПро)
- Континент (Код Безопасности)
- DiSec VPN (Фактор-ТС)
- ViPNet Client (Инфотекс)
- S-Terra VPN (S-Terra)
- Застава (Элвис-Плюс)

Принцип работы решения



1. Рутокен ЭЦП 2.0 Flash подключается к USB-порту компьютера.
2. В BIOS или EFI настраивается загрузка операционной системы с USB-диска. В большинстве случаев достаточно удерживать клавишу F12.
3. Загружается операционная система Linux или Windows.
4. Пользователь выполняет строгую двухфакторную аутентификацию в ОС, вводя свой PIN-код.
5. Защищенный раздел с документами пользователя становится доступен для работы.
6. Клиент VPN устанавливает безопасное соединение с сетью организации.
7. Клиент RDP/VDI подключается к служебному ПК или к серверу виртуальных рабочих столов.
8. Используя офисное ПО, входящее в состав операционной системы, сотрудник может редактировать документы и сохранять их в защищенный раздел.
9. Документы могут быть подписаны с помощью усиленной квалифицированной электронной подписи (УКЭП). Ключи электронной подписи хранятся в защищенной памяти устройства.