СИБРУС

Описание продукта: функции и особенности

версия 1.1.

www.cybrus.ru

1. Решение СИБРУС

Назначение СИБРУС — организация защищенной корпоративной связи между сотрудниками, клиентами и партнерами компаний через локальные вычислительные сети и глобальную сеть Интернет.

Отличительные особенности СИБРУС

- Система предоставляет богатый набор средств быстрых прямых коммуникаций между пользователями для повседневной совместной работы в неформализированном формате, не являясь при этом заменой систем документооборота с регламентированными потоками документов и правил их составления и обработки.
- СИБРУС предлагает комплексное решение для максимального усиления безопасности корпоративной связи, включающее в себя разнообразный набор мер для защиты от широкого спектра угроз информационной безопасности.
- СИБРУС является российской разработкой и не требует импорта технологий и контроля со стороны зарубежных производителей программного обеспечения.

2. Основные функции СИБРУС

2.1. Текстовая переписка

- Прямая переписка между отдельными пользователями.
- Групповые чаты.
- Отложенная доставка сообщений получателям, не подключенным к серверу.
- Отложенная отправка сообщений отправителями, не подключенными к серверу.
- Возможность редактирования любого отправленного сообщения так, что оно будет изменено и на стороне получателя.
- Возможность удаления любого отправленного сообщения так, что оно будет удалено на стороне получателя.
- Возможность удаления любого принятого сообщения.
- Возможность очистки истории переписки с полным удалением сообщений как на сервере, так и на клиентских устройствах.

  - Операция полной очистки истории переписки пользователя.
  - Операция избирательной очистки истории пользователя как по произвольному диапазону дат, так и по произвольному контакту.
- Встроенная проверка орфографии при написании сообщений.
- Функция цитирования сообщений.
- Возможность вставки в сообщения ссылок на пользователей СИБРУС.
- Возможность персонального выделения сообщений в групповых чатах при обращении к конкретному участнику или участникам группового чата.
- Функция форматирования текста сообщений — подчеркивание, курсив, выделение жирным, зачеркивание.
- Режим автоматического удаления сообщений через заданный период времени.
- Групповая рассылка сообщений.
- Специальный вид интерактивных сообщений - вопросов, на которые получатель может выбрать ответ сразу же в этом сообщении.
- Отправка в сообщениях графических символов эмоций — «смайликов».

2.2. Обмен файлами

- Прямая отправка файлов от одного пользователя к другому пользователю.
- Отправка файлов в групповые чаты.
- При удалении файла отправителем этот файл также удаляется у всех его получателей.
- Отложенная отправка файлов получателям, не подключенным к серверу.
- Отложенная отправка файлов отправителями, не подключенными к серверу.
- Возможность приостановки и возобновления отправки и приема файла.
- Автоматическое восстановление докачки файла при потере и восстановлении сетевого соединения.
- Пересылка ранее отправленных или принятых файлов без необходимости их повторной отправки по сети.
- Встроенный файловый менеджер с возможностью навигации по отправленным и присланным файлам по разным контактам и периодам времени.
- Список недавних закачек файлов.
- Защищенное хранение файлов на клиентских устройствах.

  - Работа с файлами через виртуальные диски на компьютерах.
  - Работа с файлами через временные папки на мобильных устройствах.
- Три режима приема присылаемых файлов.
  - Ручной выбор принимать или не принимать файл.
  - Автоматический прием и скачивание всех присылаемых файлов.
  - Запрет на скачивание файлов на клиентское устройство, при котором файлы можно только переадресовать другому пользователю в списке контактов, но нельзя скачать на свое устройство.
- Функция записи и отправки голосовых сообщений как файлов звукового формата.
- Функция вставки изображений из буфера обмена на компьютере и отправка их как файлов графического формата.
- Отправка на компьютере одного или группы файлов путем перетаскивания мышью имен файлов из файлового обозревателя или менеджера операционной системы на контакт в списке контактов или на страницу контакта.
- Отправка изображений из галереи или с камеры на мобильных устройствах как файлы графического формата.
- Режим предварительного просмотра принятых файлов графического формата прямо в истории переписки.
- Возможность сохранения принятого и отправленного файла в любом месте на диске клиентского устройства (за исключением iOS).

2.3. Голосовая и видеосвязь

- Прямые голосовые и видео звонки между отдельными пользователями.
- Два вида групповых голосовых и видеоконференций.
  - Временные конференции, в которые любой участник может пригласить любого пользователя из своего списка контактов.
    - В конференции могут принимать участие пользователи не из своего списка контактов, а из списка контактов другого пользователя.
    - Конференция уничтожается после выхода из нее последнего пользователя.
    - Максимальное количество участников видеоконференции — 9 человек, максимальное количество участников голосовой конференции — 64 человека.
    - Для подключения и переподключения к конференции необходимо получить приглашение от участника конференции.

  - Постоянные конференции, привязанные к групповым чатам.
    - До 256 участников в конференции, из которых до 9 активных, чей голос и изображение транслируется, а остальные выступают в качестве слушателей и зрителей.
    - Конференция модерируется создателем или модераторами группового чата.
    - Любой участник группового чата может в любой момент подключиться к конференции и отключиться от нее.
    - Участник группового чата может быть подключен к конференции одновременно с нескольких своих клиентских устройств.
    - Каждый участник может включать и отключать у себя как трансляцию своего видео, так и прием видео от других участников, что актуально для плохих сетевых каналов.
- Функция изменения голоса.
- Функция удержания вызова.
- Возможность одновременной работы с большим количеством параллельных вызовов с переключением активного вызова и постановкой остальных вызовов на удержание.
- Возможность отключения микрофона и динамиков.
- Регулирование громкости микрофона и динамиков прямо в клиентской программе на компьютере.
- Функции записи, отправки и прослушивания голосовой почты.
- Два вида сетевых соединений между парами абонентов при голосовой и видеосвязи.
  - Прямой UDP-канал между абонентскими устройствами без участия сервера.
  - Трансляция данных через трансляционный сервер в случаях, когда:
    - невозможно установить прямой канал;
    - одним или обоими участниками выбрана опция скрытия IP-адреса.
  - Возможность звонков из СИБРУС на стационарные и мобильные телефоны через модуль сопряжения с SIP-сервером.
- Особенности видеосвязи.
  - Доступен полноэкранный режим видео.
  - Видео может быть выведено на дополнительный монитор, подключенный к компьютеру.

  - Три вида поддерживаемых разрешений видео:
    - низкое разрешение LD;
    - нормальное разрешение SD;
    - высокое разрешение HD.
  - Автоматическая адаптация качества видео под качество сетевого канала.
  - Возможность переключения между доступными видеокамерами во время разговора.
  - Возможность присутствия в разговоре как с трансляцией своего видео, так и с отключенной видеокамерой.

2.4. Список контактов

- Два режима просмотра списка контактов.
  - По группам.
  - По датам в порядке убывания времени недавних событий.
- Отображение контакта включает в себя.
  - Псевдоним (ник) либо имя контакта.
  - ID контакта в системе, если оно не совпадает с псевдонимом.
  - Фотографию или «аватарку» контакта.
  - Статус подключения контакта к серверу.
  - Информацию о непрочитанных сообщениях от этого контакта.
- Возможность удаления истории переписки отдельно с каждым контактом.
- Возможность выбора режима уведомлений о новых сообщениях от данного контакта или группового чата.
  - Уведомлять о всех событиях.
  - Не уведомлять ни о каких событиях.
  - Уведомлять только о тех сообщениях, которые отправлены лично мне.
- Режим скрытия отдельных контактов при котором контакт появится в списке только после ввода специального кода.
- Возможность блокировки контакта с занесением его в черный список.
- Возможность назначения режима отправки состояния видимости контакту.
  - Нормальный режим — контакт видит статусы моего подключения к серверу.
  - Всегда видим — контакт видит состояние моего подключения к серверу

даже в случае, если я перешел в режим «Невидим».

  - Всегда невидим — контакт не может отслеживать мои подключения к серверу, для него я будет всегда не подключен к серверу.

- Возможность индивидуального назначения статуса, который всегда будет отправлен контакту вне зависимости от моего фактического статуса (например, контакт будет всегда видеть статус «Не беспокоить» или «Отошел надолго» даже в случае, если мой фактический статус «В сети»).
- Четыре режима добавления контактов в список контактов.
  - Все могут добавлять.
  - Никто не может добавлять.
  - Может добавлять только тот, кто знает ответ на определенный вопрос.
  - Может добавлять только член той же самой Группы безопасности, что и я.
- Возможность запрета приема сообщений от неавторизированных контактов.
- Режим автоматического удаления сообщений через заданный период может задаваться как глобально для всех контактов, так и индивидуально для каждого контакта.
- Режим скрытия IP-адреса при звонках может задаваться как глобально для всех контактов, так и индивидуально для каждого контакта.
- Поиск по списку контактов.
- Контакты из своего списка контактов могут быть переданы в переписке другому контакту или в групповой чат так, что получатель сможет простым набором действий добавить их в свой список контактов.
- Пользователь может переименовывать и назначать изображения контактам в своем списке контактов на свое усмотрение.
- Для контакта может быть задана дополнительная информация, включающая в себя адрес, электронную почту, телефоны и т. д.
- К контакту могут быть привязаны заметки, события календаря и задачи.

2.5. Дополнительные сервисы

2.5.1. Менеджер паролей

- Система содержит механизмы безопасного хранения паролей и реквизитов доступа к различным сервисам, например, к ящикам электронной почты, банковским аккаунтам, пин-коды, аккаунтам социальных сетей и т. д.
- Пароли хранятся в защищенном виде как на клиентских устройствах, так и на сервере.

- При потере или выходе из строя клиентского устройства, пользователь всегда сможет восстановить базу паролей, подключившись новым устройством к серверу.
- Пароли могут быть безопасным образом переданы пользователям в списке контактов через специальный вид сообщений. Полученные таким образом пароли могут быть простой операцией добавлены в менеджер паролей.
- Пароли могут быть упорядочены по группам.

2.5.2. Заметки

- Система предлагает менеджер заметок для безопасного ведения и хранения текстовых заметок разного рода.
- Заметки могут быть прикреплены к конкретным пользователям так, что на странице пользователя можно просматривать и редактировать касающиеся его заметки.
- Заметки хранятся в защищенном виде как на клиентских устройствах, так и на сервере.

2.5.3. Органайзер

- Календарь событий и напоминаний.
  - Пользователь может добавлять в календарь информацию о событиях.
  - Каждое событие может сопровождаться напоминанием, которое будет отображено в клиенте.
    - Напоминания могут быть по дате и времени события.
    - Напоминания могут быть предварительные.
  - События могут быть двух типов.
    - Разовые в конкретную дату и время.
    - Периодические с несколькими видами периодов:
      - ежегодные;
      - ежемесячные по определенным дням месяца;
      - еженедельные по определенным дням недели;
      - ежедневные.
  - События могут быть разосланы по выбранным контактам в списке контактов так, что у данных контактов они также добавятся в календарь.
  - События, относящиеся к конкретному пользователю, можно просмотреть на страницы данного пользователя.
  - События хранятся в защищенном виде как на клиентских устройствах, так

и на сервере.

- **Задачи**
  - Пользователь может назначать и отслеживать выполнение различных задач.
  - Задачи могут быть как личные, так и совместные с одним и более контактом в списке контактов.
  - Пользователь может назначить задачу либо себе, либо пользователю из списке контактов.
  - Пользователь может назначить контролера и наблюдателей за задачей из списка контактов.
  - Задача может быть привязана к каким-то датам и отображаться в календаре на эти даты с генерацией соответствующих уведомлений.
  - Для каждой задачи может быть определен заголовок задачи, описание, статус, прогресс, потраченное время, ожидаемые и фактический сроки, а также приоритеты.
  - Часть полей задачи может редактировать только автор и контролер, остальные поля доступны для изменения также и назначенному исполнителю.
  - Сообщения об изменениях в задаче рассылаются всем пользователям, к которым она относится — исполнителю, контролеру и наблюдателем.
  - Каждая задача содержит журнал изменений и прогресса работы над задачей.
  - Задачи, относящиеся к конкретному пользователю, можно просмотреть на страницы данного пользователя.
  - Задачи хранятся в защищенном виде как на клиентских устройствах, так и на сервере.

2.6. Синхронизация данных

- Пользователь может быть подключен к серверу одновременно с нескольких клиентских устройств.

  В клиентском приложении можно просмотреть список своих подключений и, при необходимости, дистанционно закрыть любое свое клиентское приложение.
- Все принимаемые и передаваемые данные, включая текстовую переписку и файлы, а также данные дополнительных сервисов, автоматически синхронизируются между всеми клиентскими подключениями пользователя.

Файлы могут синхронизироваться по запросу, т. е. пользователь видит, что файлы есть на сервере, но на данное клиентское устройство он может их скачивать или не скачивать на свое усмотрение.

- При подключении серверу с нового устройства, пользователь может загрузить с сервера все данные своего аккаунта, включая историю переписки, файлы и т.д.

2.7. Работа с сетью

- Для связи клиентов с серверами используется TCP-соединение с защитой по TLS-протоколу.
- В целях отказоустойчивости сетевых подключений могут быть заданы дополнительные TCP-порты, через которые клиент будет пытаться подключиться к серверу.
- Для кластерных серверов клиент автоматически выбирает сервер, к которому подключаться, на основе DNS-балансировки.
- Для аудио и видеотрафика используется UDP-протокол. Возможно зафиксировать используемый диапазон UDP-портов.
- В случае невозможности прямого подключения к сети может использоваться SOCKS5 прокси-сервер как для TCP, так и для UDP протокола.
- Клиенты могут автоматически получить сетевые и прочие настройки сервера через сервис автоконфигурации клиента.

3. Механизмы безопасности

СИБРУС предлагает два набора инструментов для решения основных вопросов безопасного хранения и обмена данными.

- Защита данных от перехвата, утечки, прослушивания, кражи и т. д.
- Защита от бытовых ошибок или чрезвычайных ситуаций при работе в системе.

3.1. Защита данных

- **Что защищается.** Защищаются все данные, которыми пользователи обмениваются в рамках поддерживаемых видов связи, а также данные дополнительных сервисов СИБРУС, включая:
  - текстовая переписка;

- файлы;
- голосовая и видеосвязь;
- голосовые и видеоконференции;
- задачи;
- напоминания;
- заметки;
- записи менеджера паролей.

- **Как защищается.** Для защиты данных СИБРУС использует стойкие алгоритмы криптографии, сочетающие симметричное и асимметричные шифрование.
  - Возможна интеграция с сертифицированными в РФ СКЗИ.
  - В СИБРУС шифрование данных производится всегда на клиентском устройстве, и ключи шифрования доступны только самому пользователю. В сеть и на сервер данные поступают уже в зашифрованном виде, и только пользователь может расшифровать данные. Поэтому никто посторонний, даже операторы и администраторы серверов, не могут перехватить или раскрыть данные пользователя.

    Абонентским шифрованием end-to-end encryption шифруются все виды данных, включая текстовую переписку, файлы, групповые чаты, аудио- видеосвязь, а также аудио и видеоконференции.
- **Где защищается.** СИБРУС обеспечивает защиту данных на всех трех участках их передачи и хранения.
  - Компьютер или мобильное устройство пользователя.
    - Все данные на клиентском устройстве хранятся в зашифрованной базе данных.
    - Все файлы на клиентском устройстве хранятся в зашифрованном виде и доступны через виртуальные диски на компьютере или специальные временные папки на мобильном устройстве.
  - Сетевые каналы связи.
    - Связь осуществляется через защищенные каналы, в которых весь трафик между абонентами шифруется:
      - для защиты клиент-серверных соединений используются соединения TLS;
      - для защиты трафика абонент-абонент используется абонентское шифрование в режиме end-to-end encryption.

- Серверы СИБРУС.
  - Данные на серверы поступают и хранятся там уже в зашифрованном виде.
  - Для защиты данных используется абонентское шифрование end-to-end encryption так, что их невозможно расшифровать на сервере.

3.2. Дополнительные механизмы защиты от поведенческих и прочих угроз информационной безопасности.

- **Защита от кейлоггеров** (враждебного программного обеспечение, которое может перехватывать введенный текст с клавиатуры и отправлять его злоумышленнику).
  - В СИБРУС для защиты от таких программ реализована специальная виртуальная экранная клавиатура. Наиболее ценные данные пользователь может вводить с использованием данной клавиатуры. Ввод текста с такой клавиатуры осуществляется путем нажатия мышкой на соответствующие клавиши на экране.
  - Для защиты от перехвата нажатий мышки виртуальная клавиатура может после ввода каждой буквы случайным образом перемешивать расположение клавиш.
- **Просмотр и дистанционное закрытие своих подключений**.
  - СИБРУС позволяет подключаться к серверу одновременно с нескольких компьютеров или мобильных устройств. Каждое такое подключение отображается в списке подключений пользователя с указанием IP-адреса.
  - Пользователь может дистанционно отключить любое из своих подключений в списке. Например, это может быть полезно в случае, если пользователь забыл выйти из программы на работе или дома, чтобы никто в его отсутствие не смог воспользоваться программой.
- **Автоматическая блокировка или выход из программы**.
  - СИБРУС позволяет производить автоматическую блокировку или выход из программы по заданному событию. Событием может быть отсутствие активности в течение некоторого времени или отсутствие связи с сервером в течение некоторого времени.
  - При блокировке клиентская программа СИБРУС остается запущенной, но чтобы прочитать сообщения и продолжить работу с программой, необходимо ввести код разблокировки.
  - При автоматическом выходе из программы СИБРУС происходит закрытие профиля пользователя и выход из программы. Чтобы заново открыть программу необходимо ввести секретную фразу пользователя.

- **Подменная секретная фраза.**
  - Подменная секретная фраза позволяет защитить данные от доступа посторонних даже в случае, если пользователя заставляют открыть СИБРУС под принуждением.
  - При вводе подменной секретной фразы вместо штатного открытия профиля пользователя и расшифровки данных, будет выполнено одно из заранее выбранных действий:
    - некорректное завершение программы — программа будет выдавать сообщение об ошибке и перезапускаться;
    - удаление всех данных пользователя в СИБРУС на компьютере и некорректное завершение программы.
- **Избирательное редактирование сообщений и удаление истории.**
  - Если история переписки содержит сообщения, которые необходимо уничтожить, чтобы они ни в каком случае не стали известны посторонним, то СИБРУС предлагает для этого несколько вариантов. Каждый из вариантов, при этом, позволяет удалить только избранные данные, оставив остальные данные как есть. В СИБРУС пользователь может:
    - отредактировать уже отправленное сообщение — сообщение будет отредактировано как у отправителя, так и у получателя;
    - удалить отправленное сообщение или файл — сообщение или файл будут удалено как у отправителя, так и у получателя;
    - удалить принятое сообщение или файл — сообщение или файл будут удалено только у получателя;
    - удалить историю переписки за любой период для любого пользователя — история будет удалена только у самого пользователя.
- **Автоматическое удаление отправленных и принятых файлов и сообщений** через заданный период времени.
  - Режим может включаться глобально для всей переписки.
  - Режим может включаться индивидуально для каждого контакта.
- **Скрытие IP-адреса при аудио и видеосвязи.**
- **Управление списками контактов** (см. подробнее п. Список контактов).
  - Настройки режима поиска и добавления в список контактов.
  - Черный список контактов.
  - Скрытые контакты.

  - Индивидуальные настройки видимости.
  - Индивидуальные настройки статусов.
  - Индивидуальные настройки режима скрытия IP-адреса.
  - Индивидуальные настройки режима автоматического удаления сообщений.
- **Специальный «онлайн-режим» работы**, при котором запустить клиентское приложение и получить к данным, хранящимся в локальной копии СИБРУС на данном устройстве, можно только после подключения к серверу.
  - Режим эффективно использовать для возможности оперативного централизованного управления доступом пользователей к данным СИБРУС, в том числе и хранящимся локально на клиентский устройствах.
- **Возможность поставки программного обеспечения с брэндированием** и стилем заказчика (White Label). Изменение названия программного обеспечения затрудняет поиск и использование уязвимостей данного ПО, что дополнительно повышает безопасность использования такого программного обеспечения.

4. Администрирование

Администрирование системы СИБРУС включает в себя операции двух типов.

- Техническое администрирование серверов СИБРУС.
- Управление пользователями и параметрами безопасности пользователей.

4.1. Техническое администрирование

- Осуществляется системным администратором через стандартную консоль в составе операционной системы сервера.
- Включает в себя следующие операции.
  - Установка серверного программного ПО с использованием инструкций и установочных сценариев.
  - Управление лицензиями серверного ПО.
  - Управление резервированием данных.
  - Управление мониторингом работы серверов.
  - Управление обновлениями клиентского ПО.

4.2. Управление пользователями

- Осуществляется управляющим менеджером или администратором безопасности через специальный модуль расширения с графическим

интерфейсом в составе клиентского ПО на компьютерах с операционными системами Windows/Linux/Mac OSX.

- Группы пользователей сервера могут входить в состав различных Групп безопасности сервера, для каждой из которых назначен свой администратор безопасности.

  Управление пользователями разных Групп безопасности осуществляется независимо друг от друга.

- Управление пользователями включает в себя следующие операции.
  - Добавление и удаление пользователей.
  - Задание песевдонима (никнейма), ФИО, изображения и прочих данных пользователя.
  - Централизованное назначение настроек, специальных режимов и функций безопасности пользователей.
  - Назначение ключей шифрования, секретных фраз, паролей и секретных кодов пользователям.
  - Управление списками контактов пользователей.
  - Удаление данных пользователя.
  - Просмотр активных подключений пользователя с возможностью:
    - отключения пользователя от сервера;
    - дистанционного закрытия клиентского приложения.
  - Просмотр журнала подключений и активности пользователей.

5. Состав программного обеспечения

В состав программного обеспечения СИБРУС входит комплект клиентского и серверного программного обеспечения.

5.1. Клиентское программное обеспечение доступно на платформах:

- Компьютеры с операционными системами:
  - Windows;
  - Linux;
  - Mac OSX.
- Мобильные устройства с операционными системами:
  - Android;
  - iOS.

5.2. Серверное программное обеспечение доступно на платформах:

- Linux;
- Windows.

Поставляется в двух вариантах пакетов программного обеспечения:

- СИБРУС Офис - одиночный сервер для небольших групп и компаний.
- СИБРУС Предприятие - кластерное решение с неограниченными возможностями по горизонтальному масштабированию платформы.

Состав пакетов серверного ПО

- Основные серверные процессы.
- Модули, встроенные в серверные процессы:
  - модуль подключения к SIP-серверу.
  - модуль взаимодействия с внешними системами через JSON-HTTP.
- Балансировщик нагрузки между процессами.
- Медиаретранслятор и видеосервер для аудио и видеосвязи.
- Модуль поддержки кластеризации.
- Модуль междоменного взаимодействия для связи пользователей разных независимых серверов друг с другом.
- Модуль мониторинга с возможностью интеграции с внешними системами мониторинга (например, Zabbix).
- Дополнительные кастомизированные модули для решения различных задач централизованного управления с использованием системы СИБРУС, например:
  - Web-модуль самостоятельной регистрации и восстановления паролей пользователей;
  - Web-модуль «Красная кнопка» для быстрой остановки сервера по кнопке с любого устройства через браузер;
  - модуль управления авторизацией пользователей через СИБРУС в сторонних системах (в частности, на сервере терминалов Windows).

5.3. Схема лицензирования серверного ПО

- Серверное ПО лицензируется в расчете на количество пользовательских аккаунтов на сервере.
- Лицензия предоставляется на подписочной ежегодной основе и включает в себя бесплатные обновления как клиентского, так и серверного ПО.
  - В отдельных случаях возможны пожизненные лицензии с изолированной схемой обновления клиентского ПО.
  - Лицензия привязывается к логическому экземпляру базы данных сервера с тем, чтобы можно было выполнять прозрачный перенос серверного ПО между физическими серверами или докупать дополнительные серверы без необходимости обновления лицензии.

5.4. Дополнительно

- Возможность поставки как серверного, так и клиентского программного обеспечения под брэндом заказчика (схема White Label).
- Возможность поставки программного обеспечения, совместимого с сертифицированными в РФ СКЗИ. Существует совместное с компанией ИнфоТеКС решение с защитой сетевых каналов с помощью сертифицированных СКЗИ ViPNet.