СИБРУС

# Безопасность и технологии защиты

версия 1.1.

www.cybrus.ru

# 1. Защита данных

Безопасность — это основной принцип, на котором базируется система СИБРУС. Для безопасного хранения и обмена данными в СИБРУС предусмотрен набор инструментов для решения следующих задач:

- Защита данных от перехвата, утечки, подслушивания, кражи и т.д.
- Защищенная работа в системе в чрезвычайных ситуациях— при принуждении к открытию программы, изъятию компьютера с запущенной программой, , бегстве инсайдера с компьютером и т.д.
- Защита от кейлоггеров.

## 1.1. Что защищает СИБРУС

**СИБРУС защищает все данные, которыми пользователи обмениваются или хранят в системе, включая:**

- текстовую переписку;
- файлы;
- голосовую и видеосвязь;
- задачи;
- напоминания;
- заметки;
- записи менеджера паролей.

## 1.2. Как происходит защита

**Для защиты данных используются стойкие алгоритмы криптографии:**

- Для защиты данных пользователей используется комбинация алгоритмов симметричного и асимметричного шифрования.
- Для реализации шифрования могут использоваться сертифицированные СКЗИ.
- При использовании сертифицированных СКЗИ схемы управления шифрованием и ключами могут отличаться, с целью соответствия требованиям эксплуатации используемого СКЗИ.

Шифрование данных производится всегда на клиентском устройстве, а 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 сам провайдер сервиса, не может перехватить или раскрыть данные пользователя.

### 1.3. Где происходит защита

Защита осуществляется на всех этапах передачи и хранения данных.

| **Участок** | **Как защищается** |
|---|---|
| Компьютер или мобильное устройство пользователя | 1. Вся данные на клиентском устройстве хранятся в зашифрованной базе данных.<br><br>2. Все файлы на клиентском устройстве хранятся в зашифрованном виде, на компьютерах файлы доступны через виртуальные диски, а на мобильных устройствах Android и iOS файлы для чтения расшифровываются во временные папки, которые после использования автоматически чистятся. |
| Каналы связи | Связь осуществляется через защищенные каналы, в которых весь трафик между пользователями шифруется. |
| Сервер СИБРУС | Данные поступают на сервер уже зашифрованными и хранятся там в зашифрованном виде. |

## 2. Дополнительные инструменты безопасности

### 2.1. 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.

### 2.2. Автоматическая блокировка или выход из программы

СИБРУС позволяет производить автоматическую блокировку или выход из программы по заданному событию. Событием может быть отсутствие активности или отсутствие связи с сервером в течение некоторого времени.

При блокировке программа остается запущенной, но, чтобы прочитать сообщения и продолжить работу, необходимо ввести код разблокировки.

При автоматическом выходе из программы происходит закрытие профиля пользователя и выход из программы. Чтобы заново открыть программу, необходимо ввести секретную фразу пользователя.

Инструменты блокировки могут быть полезны для предотвращения доступа посторонних к программе в отсутствие пользователя, когда он оставил программу запущенной или отлучился.

Также эти инструменты позволяют защитить данные пользователя, если у него отняли работающий компьютер с запущенной программой. В этом случае у злоумышленников будет только ограниченное время, чтобы успеть изучить данные программы.

## 2.3. Подменная секретная фраза

Подменная секретная фраза позволяет защитить данные от доступа посторонних даже в случае, когда пользователя принуждают открыть программу. При вводе подменной секретной фразы, вместо штатного открытия профиля пользователя и расшифровки данных, будет выполнено одно из заранее выбранных действий:

- некорректное завершение работы программы — программа будет выдавать сообщение об ошибке и перезапускаться;
- удаление всех данных пользователя в программе на компьютере и некорректное завершение работы программы.

## 2.4. Редактирование сообщений и удаление истории

Если история переписки содержит сообщения, которые необходимо уничтожить, чтобы они не стали известны посторонним, то СИБРУС предлагает для этого несколько вариантов.

Каждый из вариантов позволяет удалить только избранные данные, оставив остальные данные как есть.

**Пользователь может:**

- Отредактировать уже отправленное сообщение. Сообщение будет отредактировано как у отправителя, так и у получателя.
- Удалить отправленное сообщение. Сообщение будет удалено как у отправителя, так и у получателя.
- Удалить принятое сообщение. Сообщение будет удалено только у получателя.
- Удалить историю переписки за любой период для любого пользователя. История будет удалена только у самого пользователя.

## 2.5. Управление списками контактов

### 2.5.1. Авторизация контактов

Авторизация пользователей важна для защиты пользователей от спама и сохранения их конфиденциальности. Чтобы добавить людей в свой список контактов, их нужно авторизовать.

**Для добавления в список контактов есть три опции:**

- Разрешать всем пользователям отправлять запрос авторизации.
- Задать вопрос для потенциальных контактов.
- Запретить всем отправлять запрос авторизации.

### 2.5.2. Скрытые контакты

Контакты пользователя в СИБРУС уже защищены его паролем и секретной фразой, но можно удвоить безопасность, если настроить для части контактов дополнительные пароли – коды для разблокировки.

**Коды для разблокировки можно использовать для:**

- Контактов СИБРУС.
- Телефонных контактов.
- Групп контактов.
- Групповых чатов.

### 2.5.3.Чёрный список контактов

Если кто-либо из контактов беспокоит пользователя нежелательным общением, это контакты можно добавить в чёрный список. Контакты из чёрного списка не могут отправлять сообщения пользователю. Позже контакты из чёрного списка можно удалить и возобновить общение. Также можно настроить видимость контактов из чёрного списка – при желании их можно скрыть.

### 2.5.4. Настройки видимости пользователя

Пользователь СИБРУС может настроить видимость своего статуса подключение не только для всех, но и для конкретных контактов.

**Пользователь может выбрать:**

- Кто может видеть его реальный статус подключения.
- Кто постоянно будет видеть статус «Не в сети».
- Кто будет видеть его всегда онлайн, даже если текущий статус – «Невидим».

### 2.5.5.Настройка уведомлений

Пользователи могут настроить оповещение о входящих сообщениях в личной переписке и в групповых чатах.

**Для уведомлений есть три опции:**

- Показывать все входящие сообщения.
- Показывать только те сообщения, где отмечен пользователь.
- Отключить уведомления.

Уведомления настраиваются независимо на разных устройствах.

## 2.6. Защита от кейлоггеров

Кейлоггер — это враждебное программное обеспечение, которое может перехватывать введенный текст с клавиатуры и отправлять его злоумышленнику.

Для защиты от таких программ в СИБРУС 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 случайным образом перемешивать расположение клавиш после ввода каждой буквы.

## 2.7. Управление пользователями в рамках групповых аккаунтов

Владелец группового аккаунта может централизованно управлять настройками безопасности всех пользователей этого аккаунта. Владелец может задавать пользователям пароли, секретные фразы,

блокировки и т. п. Кроме того, он может удалять историю и блокировать пользователей группового аккаунта.

В рамках групповых аккаунтов предусмотрен специальный механизм для защиты от бегства инсайдеров с компьютером. Механизм не гарантирует абсолютную защиту от утечки данных с инсайдером, но может повысить степень защищенности от такого вида угроз.

Пользователю группового аккаунта может быть назначен специальный режим работы, при котором он может работать с программой СИБРУС только тогда, когда он подключен к серверу.

Таким образом, пользователь не сможет открыть локальный профиль пользователя и запустить программу, если у него нет подключения к серверу. Расшифровать локальные данные на компьютере такого пользователя без подключения к серверу также невозможно, т. к. для расшифровки необходимо получить специальный секрет-маску с сервера. Если пользователь запустил программу СИБРУС, когда он еще не был заблокирован, а потом просто отключился от сервера, то по истечении заданного периода времени программа автоматически закрывается.

Данный механизм гарантирует, что в случае блокировки пользователя на сервере, этот пользователь не сможет прочитать даже те данные, которые уже находятся на его компьютере.

# 3. Криптографическая защита данных

В СИБРУС все данные, подлежащие защите, передаются и хранятся в зашифрованном виде. Для шифрования данных используются стойкие алгоритмы шифрования:

- Для защиты данных пользователей используется комбинация алгоритмов симметричного и асимметричного шифрования.
- Для реализации шифрования могут использоваться сертифицированные СКЗИ.
- При использовании сертифицированных СКЗИ схемы управления шифрованием и ключами могут отличаться, чтобы соответствовать требованиям эксплуатации используемого СКЗИ.

## 3.1. Управление ключами шифрования

Степень защиты данных определяется не только используемым алгоритмом шифрования, но и тем, как создаются, хранятся и передаются секретные ключи шифрования.

**Отличительной особенностью СИБРУС является система управления ключами шифрования**. Вся безопасность СИБРУС строится на том, что только пользователь имеет доступ к ключам расшифровки его данных, поэтому никто посторонний, даже сам разработчик, не может прочитать данные пользователя, которые передаются и хранятся в системе.

**Основные виды ключей и секретов, с которыми работает СИБРУС**

| Ключ / секрет | Назначение | Происхождение | Хранение | Доступ |
|---|---|---|---|---|
| Пароль пользователя. | Доступ клиента к серверу СИБРУС. | Выбирается в момент создания аккаунта или при смене пароля. | 1. В хэшированном виде на сервере.<br>2. В хэшированном виде на компьютере в зашифро- | 1. Пользователь.<br>2. Сервер. |

| | | | | |
|---|---|---|---|---|
| | | | ванной базе данных. | |
| Разовый ключ симметричного шифрования защищенного контейнера СИБРУС. | Шифрование защищаемых данных с использованием симметричного алгоритма шифрования. | Генерируется автоматически для каждого защищенного контейнера. | В зашифрованном виде в защищенном контейнере. | 1. Отправитель защищенного контейнера.<br>2. Получатели защищенного контейнера. |
| Открытый ключ пользователя. | Шифрование разовых ключей симметричного шифрования защищенных контейнеров СИБРУС. | Генерируется пользователем одновременно с секретным ключом в момент создания профиля. | 1. На сервере.<br>2. На компьютере пользователя.<br>3. В списках контактов пользователей. | Все пользователи из списка контактов. |
| Секретный ключ пользователя. | 1. Расшифровка разовых ключей симметричного шифрования защищенных контейнеров СИБРУС.<br>2. Расшифровка прочих данных, зашифрованных асимметричным алгоритмом с использованием открытого ключа пользователя. | Генерируется пользователем одновременно с открытым ключом в момент создания профиля. | 1. В зашифрованном виде на сервере.<br>2. В зашифрованном виде на компьютере пользователя. | Только сам пользователь. |
| Секретная фраза пользователя. | Расшифровка секретного ключа пользователя. | Задается пользователем в момент создания профиля. | Нигде не хранится | Только сам пользователь. |

## 3.2. Хранение данных

Все данные, как на компьютерах пользователей, так и на сервере, хранятся в зашифрованном виде.

| **Данные** | **Передача** | **Хранение** | |
|---|---|---|---|
| | | **Сервер** | **Компьютер** |
| Текстовая переписка | Защищенный контейнер СИБРУС | Защищенный контейнер СИБРУС | Зашифрованная база данных СИБРУС |
| Данные дополнительных сервисов: органайзер, менеджер паролей, заметки | Защищенный контейнер СИБРУС | Защищенный контейнер СИБРУС | Зашифрованная база данных СИБРУС |

| | | | |
|---|---|---|---|
| Голосовая и видеосвязь | Защищенные каналы СИБРУС | - | - |
| Файлы | Зашифрованные блоки специального формата СИБРУС | Зашифрованные блоки специального формата СИБРУС | Зашифрованные блоки специального формата СИБРУС |

### 3.2.1. Защищенный контейнер СИБРУС

Защищенный контейнер СИБРУС является основным форматом данных, в котором происходит обмен зашифрованной информацией между пользователями. Все сообщения передаются и хранятся на сервере в защищенных контейнерах.

Контейнер СИБРУС включает в себя блоки симметричного и асимметричного шифрования и построен по принципу, подобному тому, который используется для защиты писем S/MIME.

Исходное сообщение шифруется симметричным алгоритмом на разовом ключе шифрования. Сам разовый ключ шифрования затем зашифровывается асимметричным алгоритмом на открытых ключах отправителя и получателей сообщения. Соответственно, только отправитель и получатели могут расшифровать сначала разовый ключ с помощью своих секретных ключей, а затем и само сообщение.

**Защищенный контейнер**

| **ID отправителя** | **ID получателя** | |
|---|---|---|
| Разовый ключ симметричного шифрования, зашифрованный асимметричным алгоритмом с использованием открытого ключа отправителя. | Разовый ключ симметричного шифрования, зашифрованный асимметричным алгоритмом с использованием открытого ключа получателя. | Защищаемые данные, зашифрованные симметричным алгоритмом с использованием разового ключа симметричного шифрования контейнера. |

### 3.2.2. Зашифрованная база данных на компьютере

На компьютерах и мобильных устройствах пользователей история переписки и прочая информация хранится в локальной зашифрованной базе данных. База данных шифруется симметричным алгоритмом.

Мастер-ключ шифрования базы данных генерируется в момент создания базы и хранится только на этом же компьютере. Ключ хранится в зашифрованном виде. Для расшифровки ключа используется секретная фраза и секретный ключ пользователя.

**Зашифрованная база данных на компьютере**

| **Формат** | **Управление ключами** | **Доступ** |
|---|---|---|
| Каждая страница базы данных зашифрована симметричным алго- | 1. Мастер-ключ симметричного шифрования генерируется в момент создания профиля пользователя на компьютере.<br>2. На основе мастер-ключа генерируются разовые ключи | 1. На каждом компьютере мастер-ключ свой, т.е. локальная база одного и того же пользователя на разных компьютерах зашифрована по-разному.<br>2. Доступ к мастер-ключу имеет только сам пользователь на данном компьютере: |

| | | |
|---|---|---|
| ритмом на разовом ключе. | для шифрования каждой страницы базы данных.<br>3. Мастер-ключ хранится на компьютере пользователя и зашифрован асиммет-ричным алгоритмом на открытом ключе пользовате-ля.<br>4. На сервер мастер-ключ никог-да не передается. | мастер-ключ расшифровывается с использованием секретного ключа после ввода секретной фразы пользователя.<br>3. В групповом аккаунте возможен режим, когда пользователю разрешен доступ к локальной базе данных только после подключения к серверу. В этом случае мастер-ключ дополнительно маскируется маской доступа, которая хранится на сервере и поступает на компьютер только после подключения к серверу. До тех пор, пока не будет подключения к серверу, невозможно узнать мастер-ключ и расшифровать базу данных. |

### 3.2.3. Защищенное файловое хранилище

СИБРУС обеспечивает одинаковую защиту всех данных, которые пользователь хранит или передает в системе. Это относится и к файлам, передаваемым в СИБРУС: файлы не только передаются зашифрованными, но и хранятся зашифрованными, как на сервере, так и на компьютере пользователя.

Для работы с зашифрованными файлами на компьютере пользователя используются специальные виртуальные диски, через которые происходит прозрачная расшифровка файлов при работе с ними из любых программ на компьютере.

**Защищенное файловое хранилище**

| Хранение | Формат | Управление ключами | Доступ |
|---|---|---|---|
| На сервере | Каждый файл разбивается на блоки, каждый блок шифруется симметричным алгоритмом с использования разового ключа шифрования. | 1. Для каждого файла генерируется мастер-ключ симметричного шифрования.<br>2. Для каждого блока файла на основе мастер-ключа формируется разовый ключ симметричного шифрования.<br>3. Мастер-ключ шифрования файла хранится и передается в защищенном контейнере с использованием открытых ключей отправителя и получателя файлов. | 1. Со стороны отправителя файла – доступ по сети на удаление и скачивание.<br>2. Со стороны получателей файла – доступ по сети на скачивание.<br>3. При удалении файла отправителем он также будет удален у всех получателей файла. |
| На компьютере* | Каждый файл разбивается на блоки, каждый блок шифруется симметричным алгоритмом с | 1. Для каждого файла генерируется мастер-ключ симметричного шифрования.<br>2. Для каждого блока файла на основе мастер-ключа форми- | 1. Доступ к файлу осуществляется через виртуальный диск. Физически файл хранится на компьютере в зашифрованном виде, |

| | | | |
|---|---|---|---|
| | использованием разового ключа шифрования. | руется разовый ключ симметричного шифрования.<br>3. Мастер-ключ шифрования файла хранится в локальной зашифрованной базе данных на компьютере пользователя. | но через виртуальный диск с ним можно работать из любой программы как с обычным незашифрованным файлом. |

* На устройствах Android и iOS файлы для чтения расшифровываются во временные папки, которые после использования автоматически чистятся.

## 3.3 Передача данных

СИБРУС защищает все передаваемые данные от перехвата и прослушивания. Помимо того, что данные уже передаются, как правило, в защищенных контейнерах, СИБРУС также дополнительно защищает сами каналы передачи данных.

**Используются каналы двух типов:**

- Соединения клиент-сервер — основное соединение с сервером СИБРУС, через которое осуществляется все клиент-серверное взаимодействие.
- прямые каналы пользователь-пользователь для голосовой и видеосвязи.

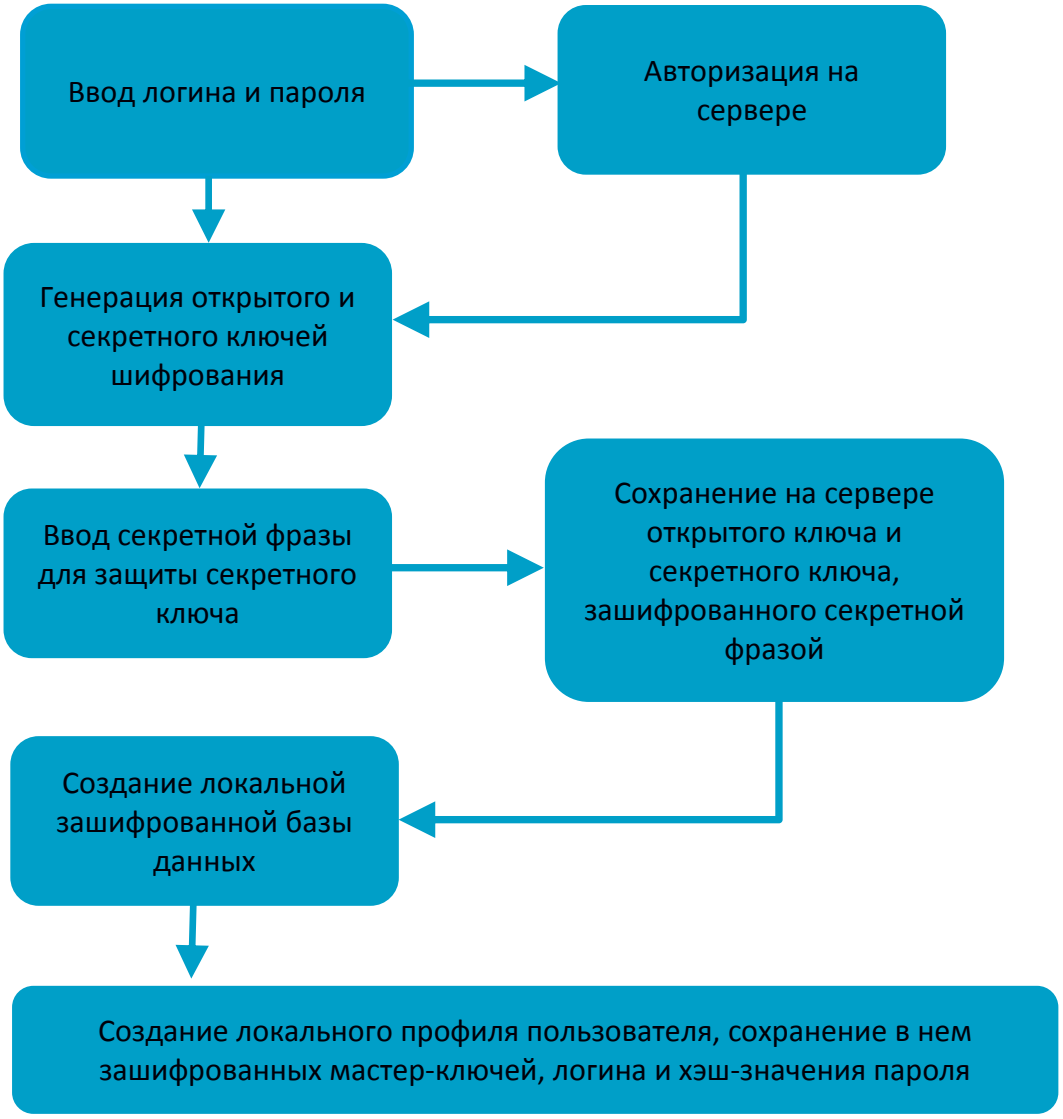
**Защищенные каналы**

| | **Вид соединения** | **Установление соединения** |
|---|---|---|
| Основное соединение с сервером. | Протокол СИБРУС через защищенное соединение TLS. | 1. Аутентификация сервера СИБРУС производится клиентом на основе сертификата сервера в стандарте X.509, заранее известного клиенту.<br>2. Авторизация клиента:<br>2.1. Клиент-серверу: запрос на подключение.<br>2.2. Сервер-клиенту: запрос авторизации с указанием случайного секрета – «соли».<br>2.3. Клиент-серверу: ответ на запрос авторизации со значением хэш, вычисленным по полученной «соли» и логину с паролем пользователя.<br>2.4. Сервер-клиенту: проверка хэш и отправка статуса авторизации клиенту. |
| Каналы для голосовой и видеосвязи. | По протоколам СИБРУС. | 1. Для каждого сеанса связи генерируется однократный ключевой материал, используемый во время сеанса для создания одноразовых ключей шифрования на каждый пакет.<br>1.1. Часть ключевого материала формируется случайным образом на каждой стороне. Данный ключевой материал |

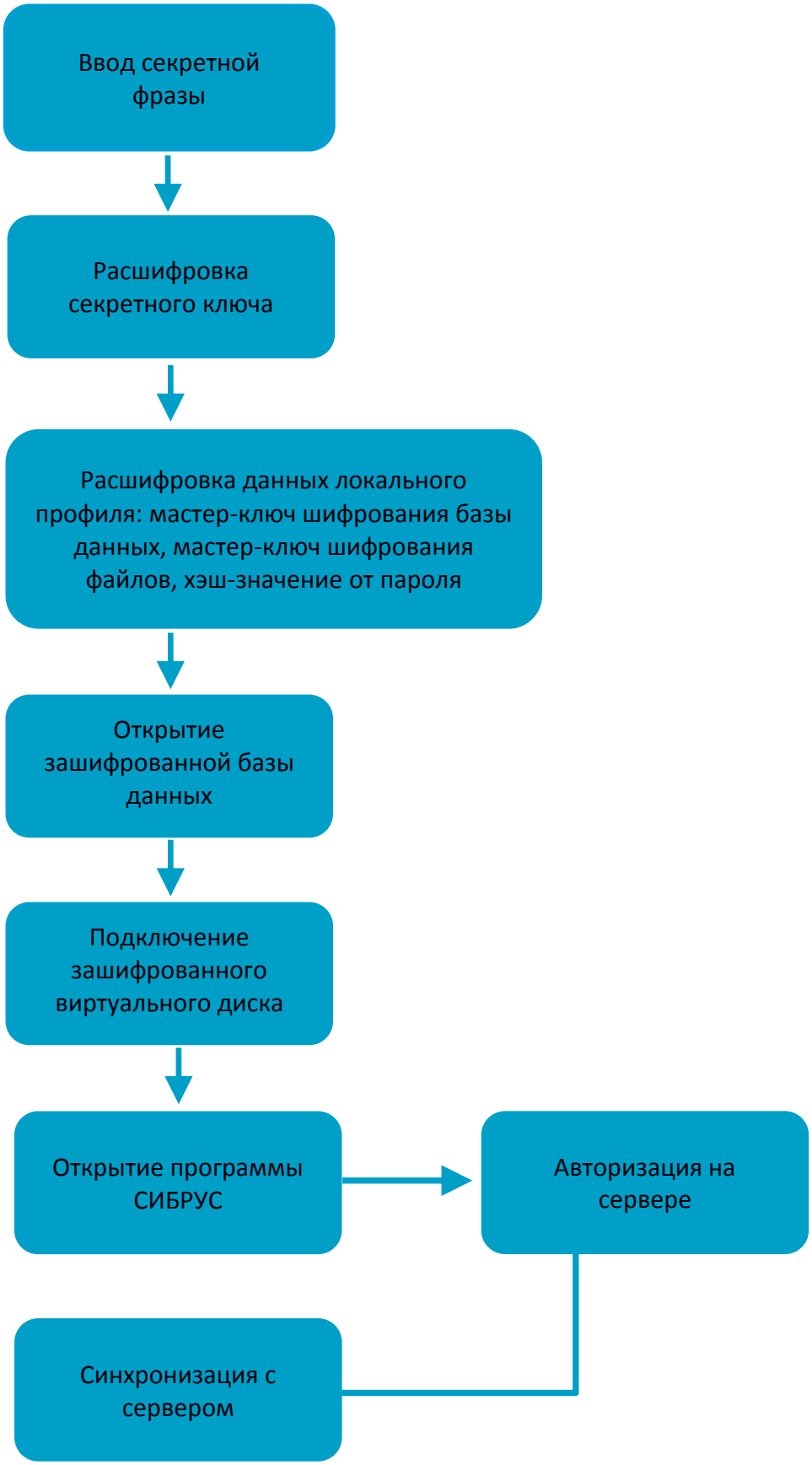
| | | |
|---|---|---|
| | | каждая сторона зашифровывает открытым ключом пользователя и передает противоположной стороне.<br>1.2. Вторая часть ключевого материала генерируется с использованием алгоритма Диффи-Хеллмана. Этот алгоритм позволяет сгенерировать ключевой материал, известный обеим сторонам, при том, что сам этот ключевой материал ни в каком виде по сети не передается.<br>2. Для каждого сетевого пакета вычисляется одноразовый ключ шифрования пакета с использованием данных пакета и ключевых материалов, сгенерированных в начале сеанса связи.<br>3. Каждый сетевой пакет шифруется симметричным алгоритмом на одноразовом ключе шифрования пакета. |

# 4. Иллюстрации механизмов защиты данных

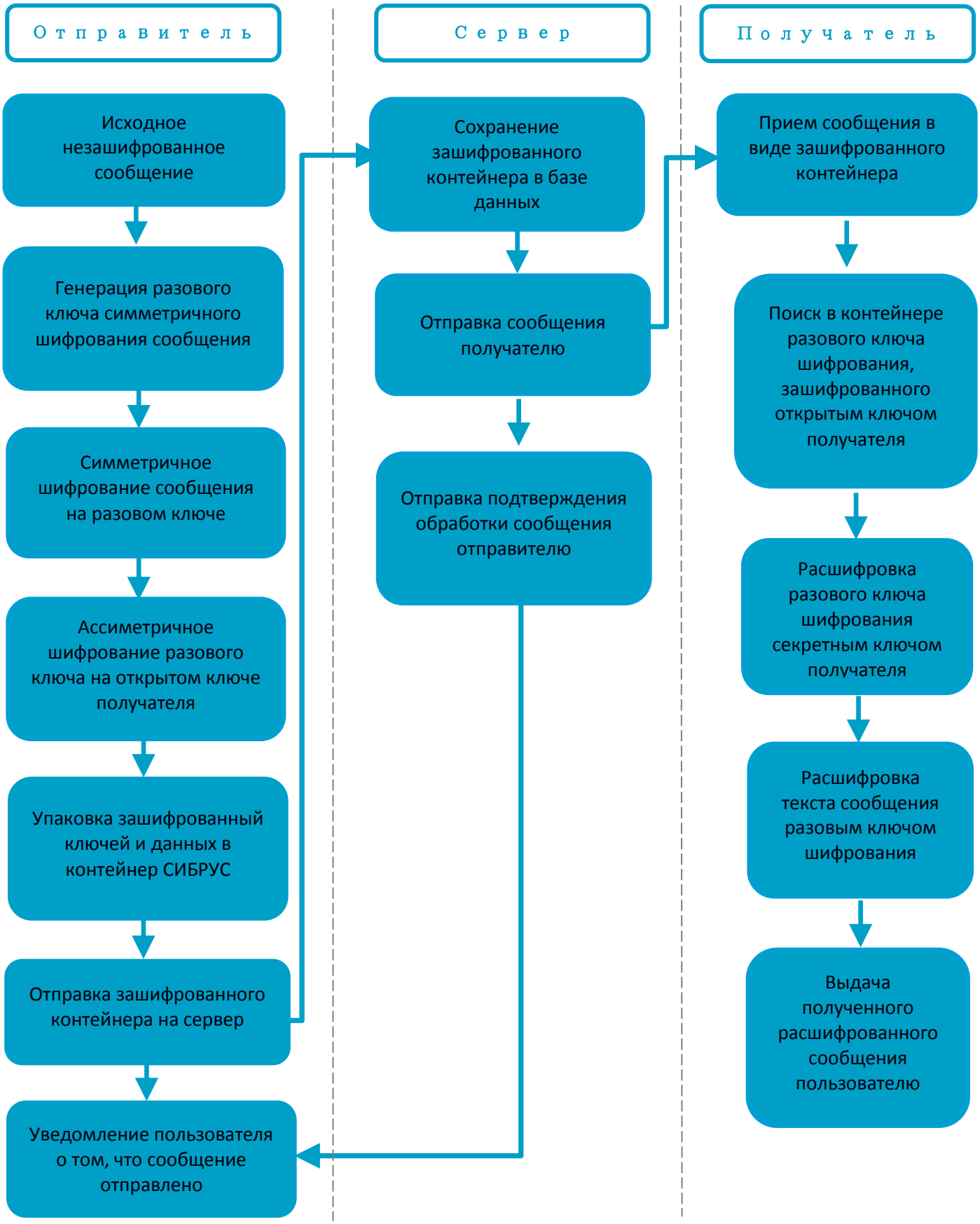
## 4.1. Создание ключей и секретной фразы пользователя, первый запуск программы



## 4.2. Штатный запуск программы СИБРУС с существующим профилем пользователя

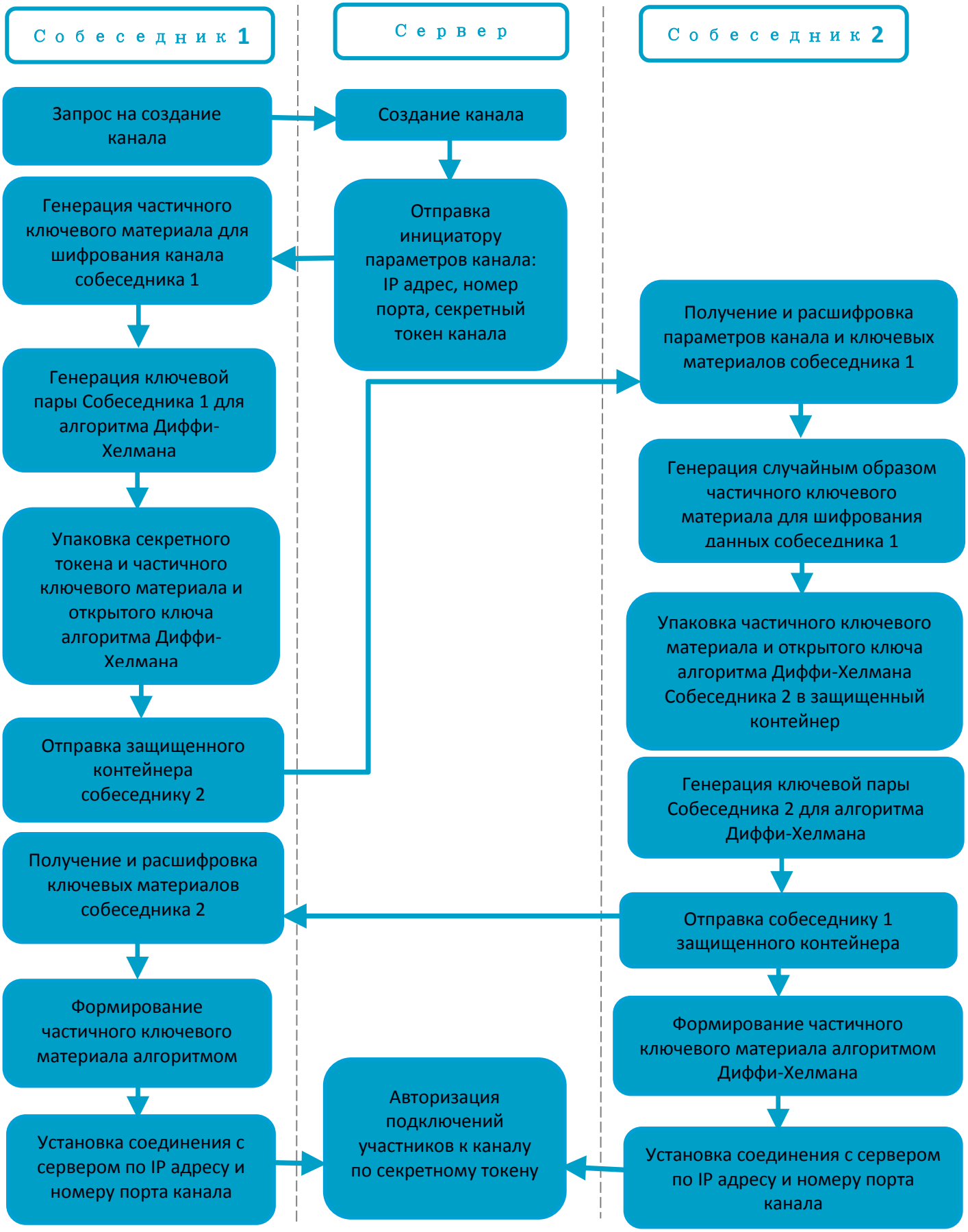


## 4.3. Обмен сообщениями между пользователями

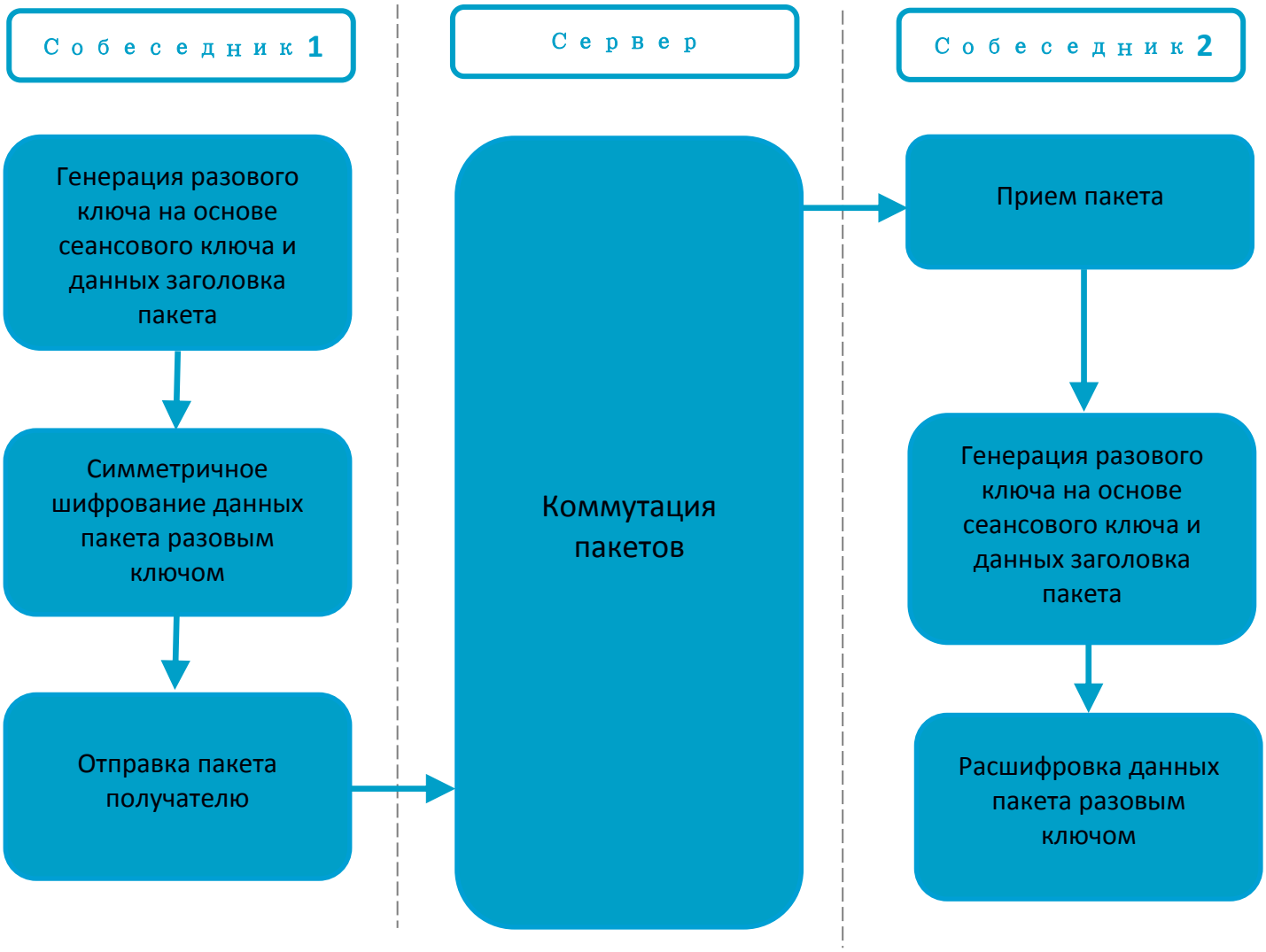


## 4.4. Защищенные каналы для аудио и видео связи

### 4.4.1 Установка соединения



### 4.4.2 Обмен пакетами через установленный канал



## 4.5 Хранение и передача файлов