

Содержание

Часть I Быстрый старт: вступление	1
1 О быстром старте	1
2 Системные требования	1
Часть II Быстрый старт: установка программы	1
1 Установка клиента для Windows	1
2 Установка в Mac OS	3
3 Переносимая (portable) версия	4
Часть III Быстрый старт: регистрация учетной записи	5
1 Первый запуск программы. Регистрация новой учетной записи	5
2 Мастер-пароль и ежедневный пароль	6
3 Визитная карточка	7
4 Криптоконтейнер	8
Часть IV Быстрый старт: знакомство с программой	10
1 Главное окно Cryptia	10
2 Настройка языка	11
3 Редактирование визитки и смена паролей	12
4 Подключение дополнительных учетных записей	13
Часть V Быстрый старт: начинаем общение	15
1 Добавление контакта	15
2 Общение	17
Часть VI Работа с учетными записями	20
1 Подключение учетной записи. Учетные записи, созданные на другом сервере.	20
2 Пары ключей	22
3 Бизнес-подключение	26
4 Автоматическое соединение с сервером	26
5 Расширенная работа с криптоконтейнером	27
Часть VII Главное окно, список контактов и история	29
1 Элементы главного окна программы	30
2 Статус соединения	32
3 Отзыв сертификатов и режим "невидимка"	33
4 Журнал сообщений	34

5	Настройки - вкладка История	35
6	Редактирование данных о контакте	36
7	Обмен визитными карточками без участия сервера	38

Часть VIII Настройки программы **39**

1	Примечание к разделу	39
2	Вкладка Интерфейс	39
3	Вкладка Аудио	41
4	Вкладка Сеть — настройка подключения и NAT	42
5	Вкладка Шифрование	43
6	Вкладка Качество речи — контроль потребляемого трафика	45
7	Вкладка Звуки событий	46

Часть IX Возможности для экспертов **47**

1	Редактирование файла Cryptia.ini	47
---	--	----

Индекс	0
---------------	----------

1 Быстрый старт: вступление

1.1 О быстром старте

Разделы, озаглавленные «Быстрый старт: ...» составляют первую логическую часть данного Руководства. Последовательное прочтение этих разделов (которое не должно занять более двадцати минут) позволит вам освоить программу Cryptia и успешно пользоваться ее основными функциями. Остальные разделы содержат более детальную информацию, описывающую не упомянутые в Быстром старте функции. Обращайтесь к ним после ознакомления с Быстрым стартом - для того чтобы получить больше контроля над вашей безопасностью или лучше понять принципы действия программы. В случае возникновения вопросов о тех или иных функциях Cryptia, рекомендуем воспользоваться поиском по данному Руководству.

1.2 Системные требования

Для установки программы Cryptia версии 9.4 на компьютер под управлением Windows вам понадобится:

- Версия Windows не ниже XP
- Не менее 512 МБ оперативной памяти и процессор с тактовой частотой не ниже 1 ГГц.

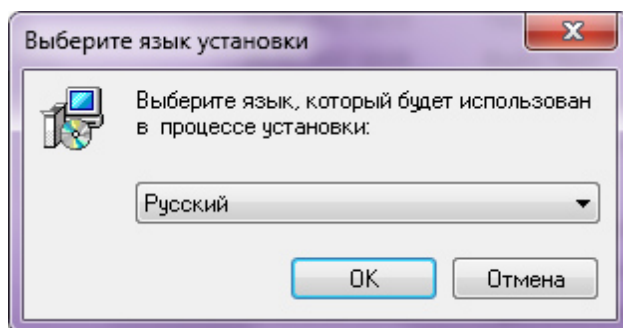
Установка на MacOS требует операционную систему Mac OS X 10.6 или новее.

Программу Cryptia можно также установить на смартфоны или планшеты - актуальную информацию о совместимости вы можете найти на сайте www.cryptia.com

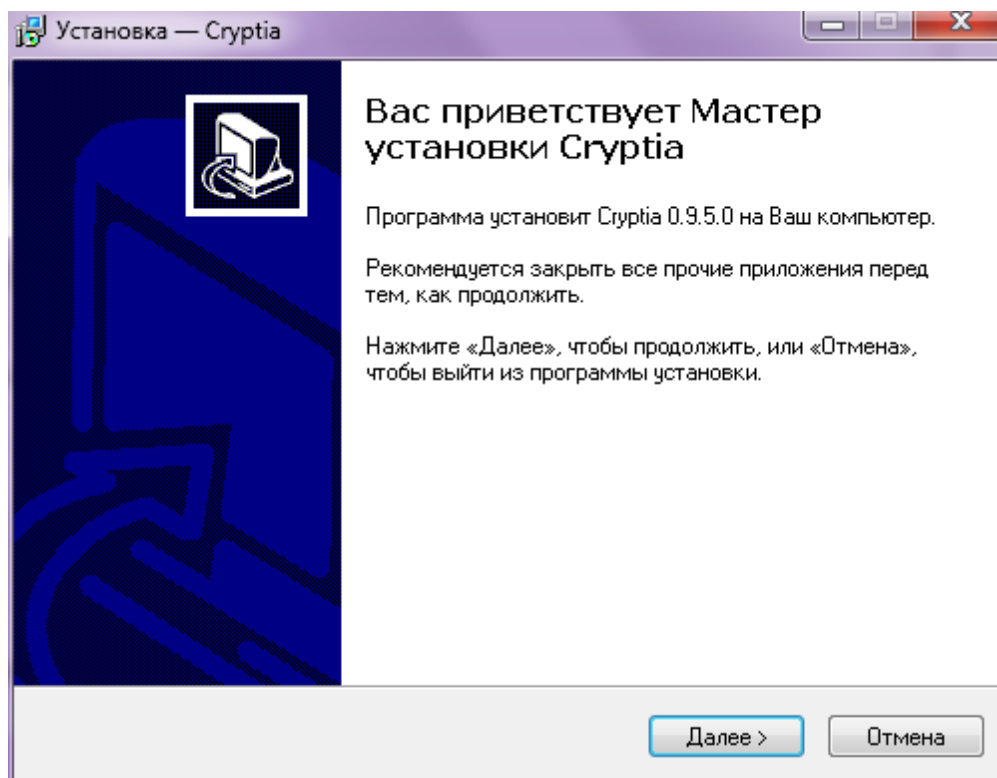
2 Быстрый старт: установка программы

2.1 Установка клиента для Windows

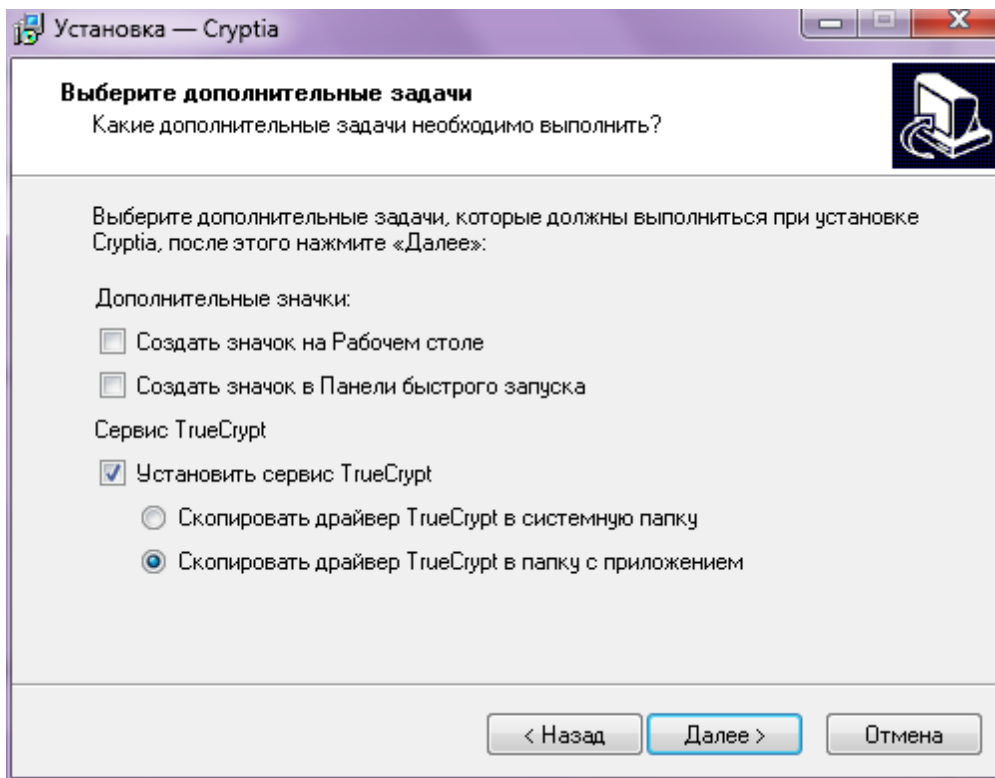
Запустите программу установки, загруженную с сайта Cryptia.com. Программа установки версии 9.4 называется cryptia_setup_win32. Этот файл вы можете найти в папке, где хранятся ваши загрузки (для Windows 7 ее обычно можно найти по адресу *C:\Пользователи\[имя пользователя]\Загрузки*) или в списке загрузок вашего браузера.



В появившемся окне выберите язык установки. Этот язык будет использоваться не только при установке программы, но и при ее запуске. Язык программы можно будет поменять и после установки (как это сделать смотрите [здесь](#)).



Далее вам понадобится прочитать и подтвердить лицензионное соглашение; указать папку, в которую будет производиться установка (проверьте, есть ли у вас права записи в желаемую папку); назвать папку в меню «Пуск»; и выбрать места, куда будут установлены ярлыки программы. За единственным исключением, процесс установки Cryptia ничем не отличается от процесса установки подавляющего большинства других программ для Windows.



TrueCrypt - это утилита, позволяющая работать с зашифрованными контейнерами (в контексте Cryptia мы будем называть их [криптоконтейнерами](#)). **Криптоконтейнер** - это виртуальный диск, который монтируется при входе в учетную запись и отключается при выходе, хранящий принятые вами файлы и обеспечивающий их шифрование. В целом, рекомендуется установить ресурсы этого сервиса, так как они позволят Cryptia создавать криптоконтейнеры и подключать их к учетным записям.

2.2 Установка в Mac OS

Смонтируйте загруженный с сайта файл cryptia_setup_mac.dmg. В открывшемся окне перетащите файл Cryptia.app на ярлык папки Applications (Приложения). Программа готова к запуску.



2.3 Переносимая (portable) версия

Программа сохраняет адресную книгу и историю в зашифрованном файле `adressbook.cdb`, а выбранные настройки программы в файле `cryptia.ini` (о дополнительных возможностях, связанных с редактированием этого файла, см. [соответствующую главу Руководства](#)).

В операционной системе Windows оба файла по умолчанию хранятся в вашей личной папке, по адресу `C:\Пользователи\[имя пользователя]\AppData\Roaming\Cryptia`.

В MacOSX файлы по умолчанию хранятся в папке, по адресу `/Users/[имя пользователя]/.config/Cryptia`.

В Linux файлы по умолчанию хранятся в папке, по адресу `/home/[имя пользователя]/.config/Cryptia`.

Если вам более по душе хранение этих файлов в папке приложения (например, с целью использования Cryptia на съемном носителе информации - флеш-устройстве или внешнем жестком диске), вы можете их переместить, создав таким образом **переносимую версию**.

Чем отличается переносимая версия? Она функционирует таким образом, что вся никакая информация не покидает пределов папки с приложением. Используя съемный носитель информации, вы можете работать с одной копией программы на разных компьютерах, и ни на одном из них не останется никаких «следов» использования Cryptia.

Ограничения переносимой версии.

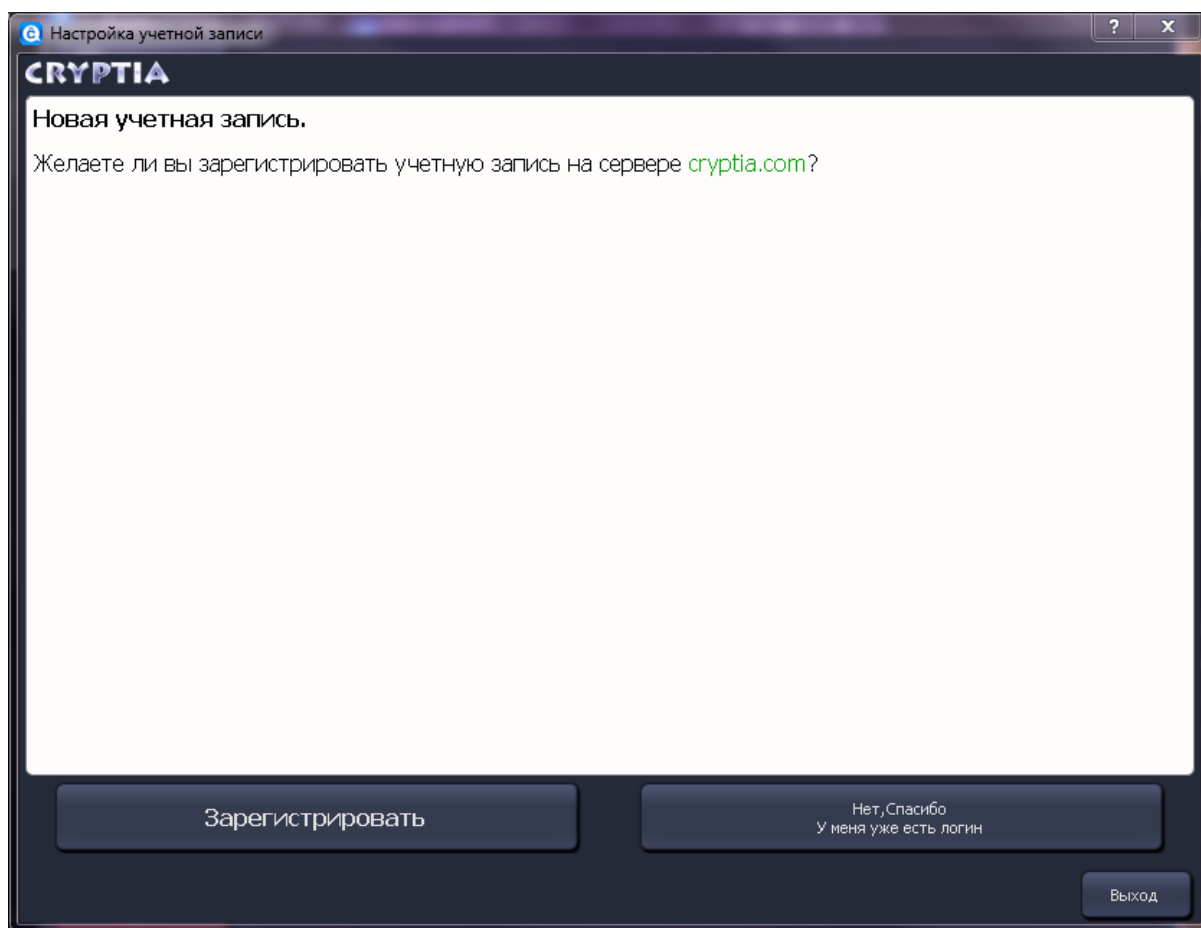
Для работы с криптоконтейнером требуется установка драйвера файловой системы, а для этого требуются полномочия Администратора (root). На всех платформах возможно работать в портативном режиме если отключить функцию криптоконтейнера. Под Windows возможно работать также и с криптоконтейнерами если у вашей учетной записи есть полномочия Администратора. Под Linux для работы портативной версии с криптоконтейнерами требуется запускать ее при помощи `sudo` с вводом пароля root. Под MacOSX такая работа невозможна.

На одном компьютере возможен единовременный запуск только одной копии программы Cryptia, так что работать одновременно с клиентом, установленным стандартным образом, и с переносимой версией не получится. Впрочем, в этом нет необходимости - Cryptia позволяет работать с несколькими учетными записями одновременно в одном окне.

3 Быстрый старт: регистрация учетной записи

3.1 Первый запуск программы. Регистрация новой учетной записи

После того, как установка прошла успешно, запустите программу. Если на этом компьютере не подключено никаких учетных записей, то перед вами откроется окно приветствия.



Так как данное руководство предназначено для использования при первом запуске, дальше мы рассмотрим процесс регистрации. Нажмите на кнопку *Зарегистрировать*.

3.2 Мастер-пароль и ежедневный пароль

Внимательно прочитайте информацию, отображаемую программой после нажатия на кнопку *Зарегистрировать*. Здесь вкратце объясняется принцип подключения к учетной записи и функции паролей: **мастер-пароля** и **ежедневного**.

Настройка учетной записи

CRYPTIA

Регистрация новой учетной записи на cryptia.com.

Укажите, пожалуйста, желаемые логин и мастер-пароль.

Если логин уже кем-то занят, о чем вы можете получить соответствующее сообщение, выберите другой.

Мастер-пароль не требуется для повседневной работы, а нужен только для восстановления доступа к учетной записи и/или экстренного отзыва всех сертификатов в случае потери доступа к вашей копии клиента Cryptia.

Поэтому мы настоятельно рекомендуем установить его достаточно сложным и сохранить в надежном месте.

Расположенный рядом с полем ввода индикатор подскажет вам, насколько сложным является ваш мастер-пароль.

Ежедневный пароль вводить необязательно.

Им зашифровывается список контактов, история сообщений, криптоконтейнер с полученными файлами и приватные ключи.

Также этот пароль требуется вводить каждый раз при установлении соединения с сервером.

Вы можете отказаться от ежедневного пароля (оставив соответствующее поле пустым) если уверены в том, что потенциальный злоумышленник не имеет возможности завладеть доступом к данной копии клиента.

Ежедневный пароль хранится локально и не передается на сервер, в то время как мастер пароль хранится только на сервере.

Логин * Введите желаемый логин здесь Максимум 20 символов. Только латинские символы цифры и символы "." и "_"

Мастер пароль * Введите мастер-пароль здесь Очень слабый 0

Повторите мастер пароль * Повторите мастер-пароль, во избежание ошибок

Ежедневный пароль Введите ежедневный пароль здесь

Повторите Ежедневный пароль Повторите мастер-пароль, во избежание ошибок

Назад Далее Выход

Запомните, что потеряв мастер-пароль, вы теряете все способы управления собственной учетной записью. Восстановить пароль или создать новый, если вы забыли существующий, невозможно. Такие меры необходимы для обеспечения адекватного уровня безопасности.

Вы можете не использовать ежедневный пароль (оставив соответствующее поле пустым), но данное решение оставит вас беззащитным перед возможным злоумышленником, если он завладеет вашей копией клиента Cryptia. Поэтому мы всё же рекомендуем установить ежедневный пароль.

Если вы пользуетесь Cryptia на нескольких устройствах, на каждом устройстве будет создан свой ежедневный пароль. При желании, вы можете их создать одинаковыми, или, например, создать ежедневный пароль на рабочем компьютере и не создавать его на домашнем.

В случае, если вы забыли ежедневный пароль или если злоумышленник получил доступ к вашей учетной записи, вы можете [отозвать все ключи](#) с помощью мастер-пароля, блокируя таким образом ежедневные пароли на всех устройствах, где подключена ваша учетная запись. Создавая новую пару ключей, вы будете иметь возможность указать новый ежедневный пароль.



The registration form is titled "Быстрый старт: регистрация учетной записи". It contains the following fields and elements:

- Логин ***: A text input field containing "ALICE". To the right, a note says: "Максимум 20 символов. Только латинские символы цифры и символы '.', ' ' и '-'".
- Мастер пароль ***: A password input field with a strength indicator bar. To the right, it says "Крепкий 73".
- Повторите мастер пароль ***: A second password input field for confirmation.
- Ежедневный пароль**: A daily password input field with a strength indicator bar. To the right, it says "Хороший 44".
- Повторите Ежедневный пароль**: A second daily password input field for confirmation.
- At the bottom right, there are three buttons: "Назад", "Далее", and "Выход".

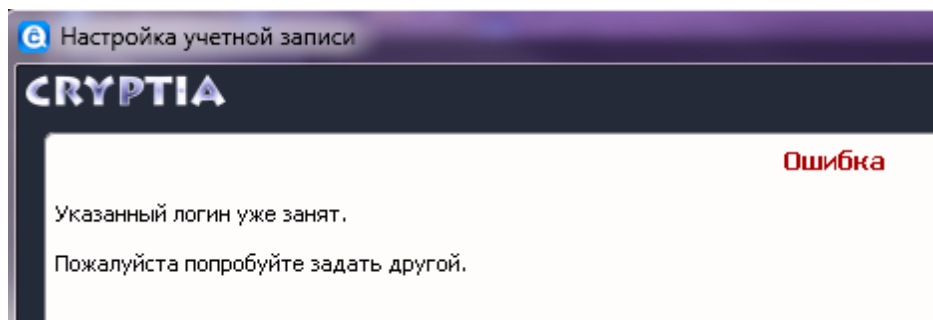
Введите логин, дважды введите мастер-пароль и дважды ежедневный. Справа от мастер-пароля находится индикатор его надежности. Пароли, использующие символы разных регистров, цифры, знаки пунктуации считаются более надёжными.

Если вы удовлетворены введенными данными, жмите *Далее*>.



Чтобы оградить сервер от роботов, при регистрации новой учетной записи необходимо ввести текст на картинке в соответствующее поле внизу. Если вам сложно прочитать картинку, попробуйте поменять ее при помощи кнопки Сменить картинку. Введя код, нажимайте *Далее*>

После успешного введения кода происходит проверка логина. Если выбранный вами логин уже занят, программа попросит создать новый.



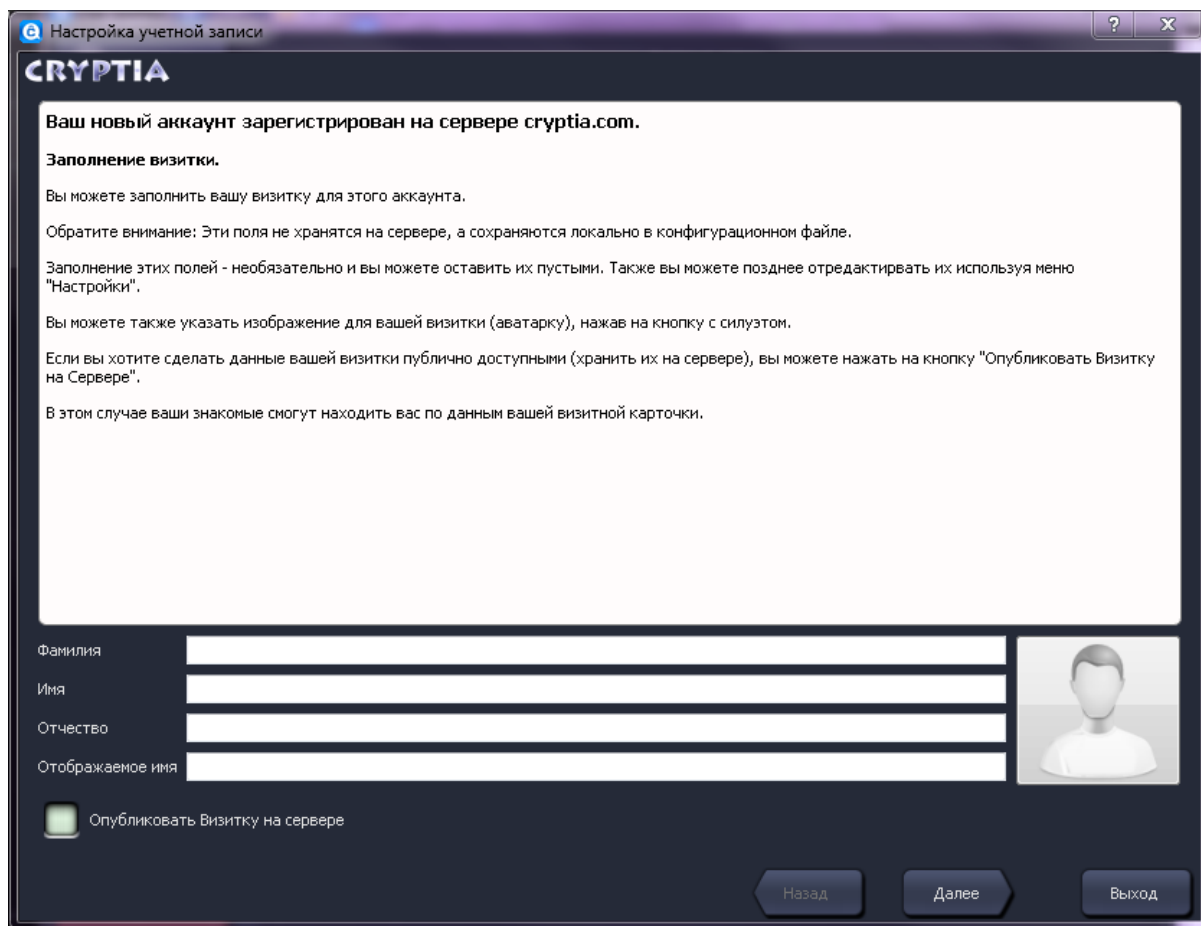
Если логин свободен, он сразу же регистрируется на сервере.

3.3 Визитная карточка

Визитная карточка — это та информация о вас, которая будет доступна другим пользователям Cryptia. Визитка включает в себя ваше имя, ваше отображаемое имя (то, как вас будут видеть другие пользователи в своем списке контактов) и любое графическое изображение (также отображаемое в списке контактов вашего собеседника). Все поля являются необязательными для

заполнения.

Передать данные вашей визитки другим пользователям можно несколькими способами. Так, если вы опубликовали свою визитку на сервере, все, кто [нашел вашу учетную запись](#) по логину, автоматически получают эти данные. Кроме того, визитку можно передать, если вы пожелаете, при установлении нового контакта, или же [записать в файл формата vCard](#) и отослать этот файл адресату электронной почтой или любым другим доступным вам способом. Имейте в виду, что пользователи, обладающие вашей визиткой, точно так же могут экспортировать данные вашей визитки в файл для передачи третьим лицам.



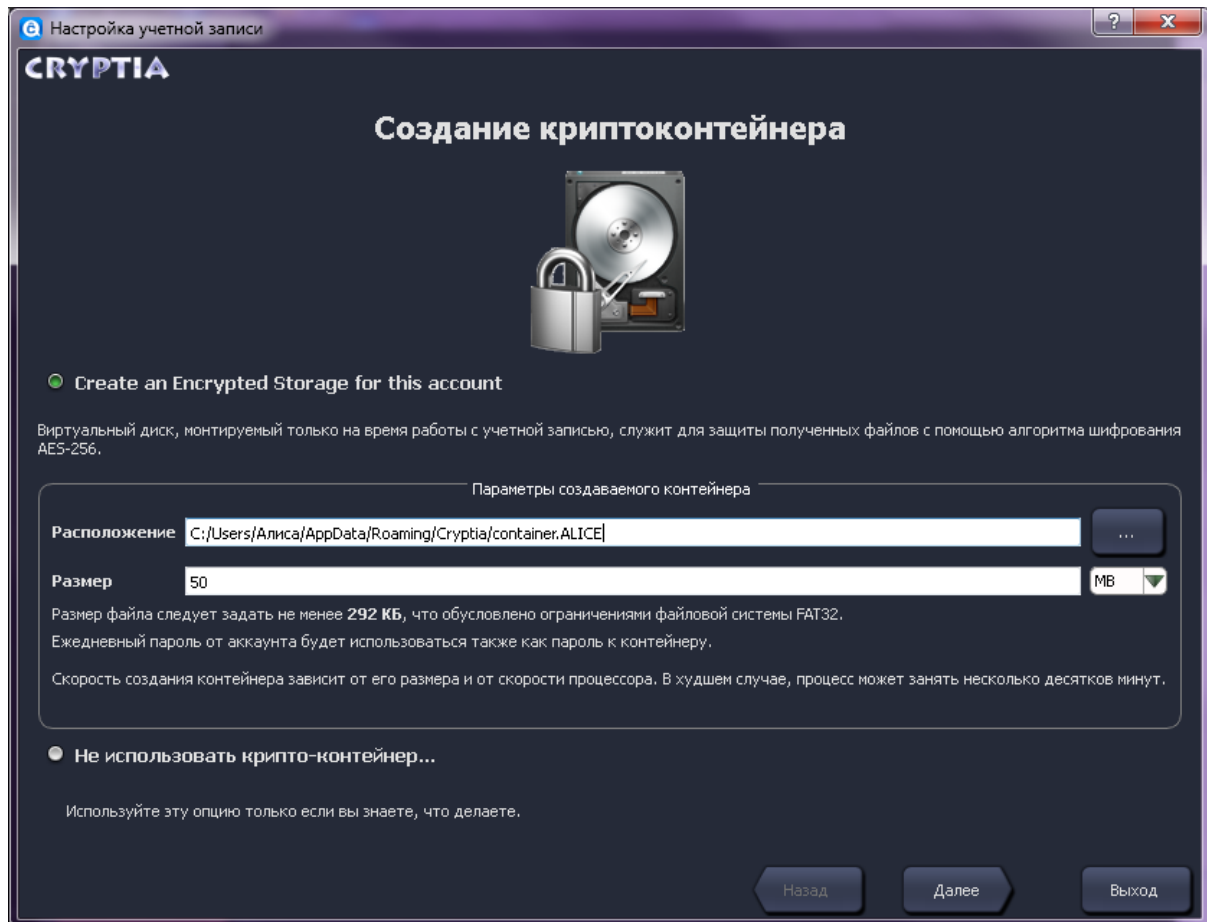
Для того чтобы добавить в визитку фотографию, или любое другое изображение, просто нажмите на кнопку со схематичным портретом справа. Вы можете пропустить шаг создания визитки, оставив все поля пустыми и нажав *Далее*>. Заполнить или отредактировать уже заполненную визитку можно в любой момент, [воспользовавшись окном настроек программы](#).

3.4 Криптоконтейнер

Последний шаг установки учетной записи связан с настройкой криптоконтейнера. Криптоконтейнер - это виртуальный диск, зашифрованный с помощью вашего ежедневного пароля и хранящий принятые вами файлы.

Этот диск монтируется (и, следовательно, появляется в списке дисков вашего компьютера - в операционной системе Windows ему чаще всего присваивается буква Z:/) каждый раз при

подключении учетной записи к серверу и отключается когда соединение прерывается. Резидентная программа CryptiaGuardian (вы можете найти ее в списке процессов вашей операционной системы) следит за своевременным размонтированием контейнера даже в случае вылета клиента Cryptia. В контейнере появляются файлы, принятые от других пользователей Cryptia и пока он смонтирован, с него (и на него) можно копировать/перемещать файлы как с любого другого диска или флешки.

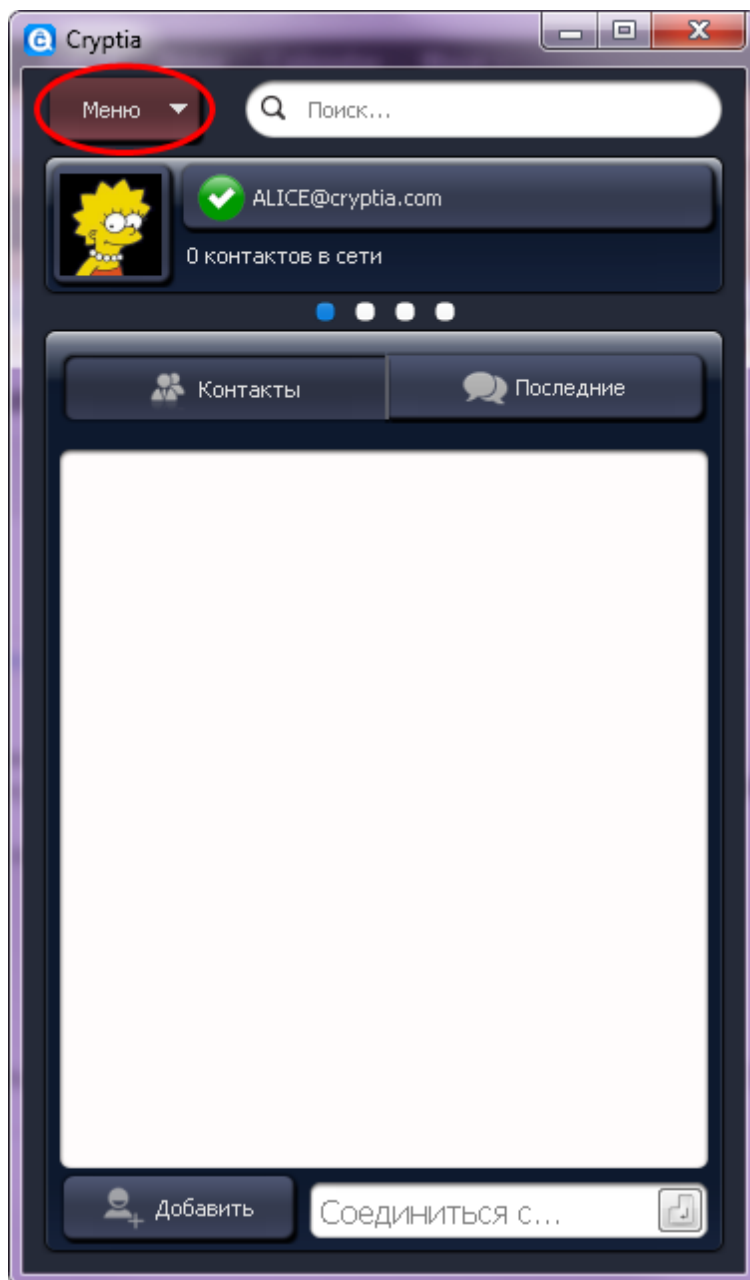


Данное окно позволяет создать криптоконтейнер, указав его расположение и размер. Учтите, что создание контейнера большого размера может занять до нескольких десятков минут - оцените, насколько большой контейнер вам нужен. 50 мегабайт, которые выставлены по умолчанию, хватает для большинства случаев. Помните, что вы можете в любой момент создать и подключить к учетной записи другой криптоконтейнер - большего размера, если в этом возникнет необходимость.

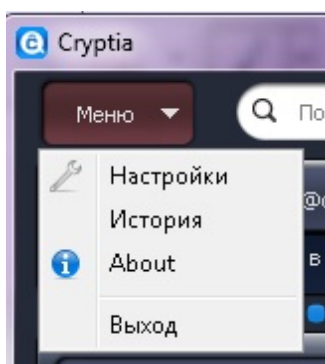
Выбирайте опцию *Не создавать криптоконтейнер* в случае, если криптоконтейнер (созданный с помощью Cryptia или утилиты [TrueCrypt](#)) у вас уже имеется - вы сможете [подключить его позже](#), из окна *Настройки*. Но учтите, что один контейнер может быть подключен лишь к одной учетной записи.

4 Быстрый старт: знакомство с программой

4.1 Главное окно Cryptia

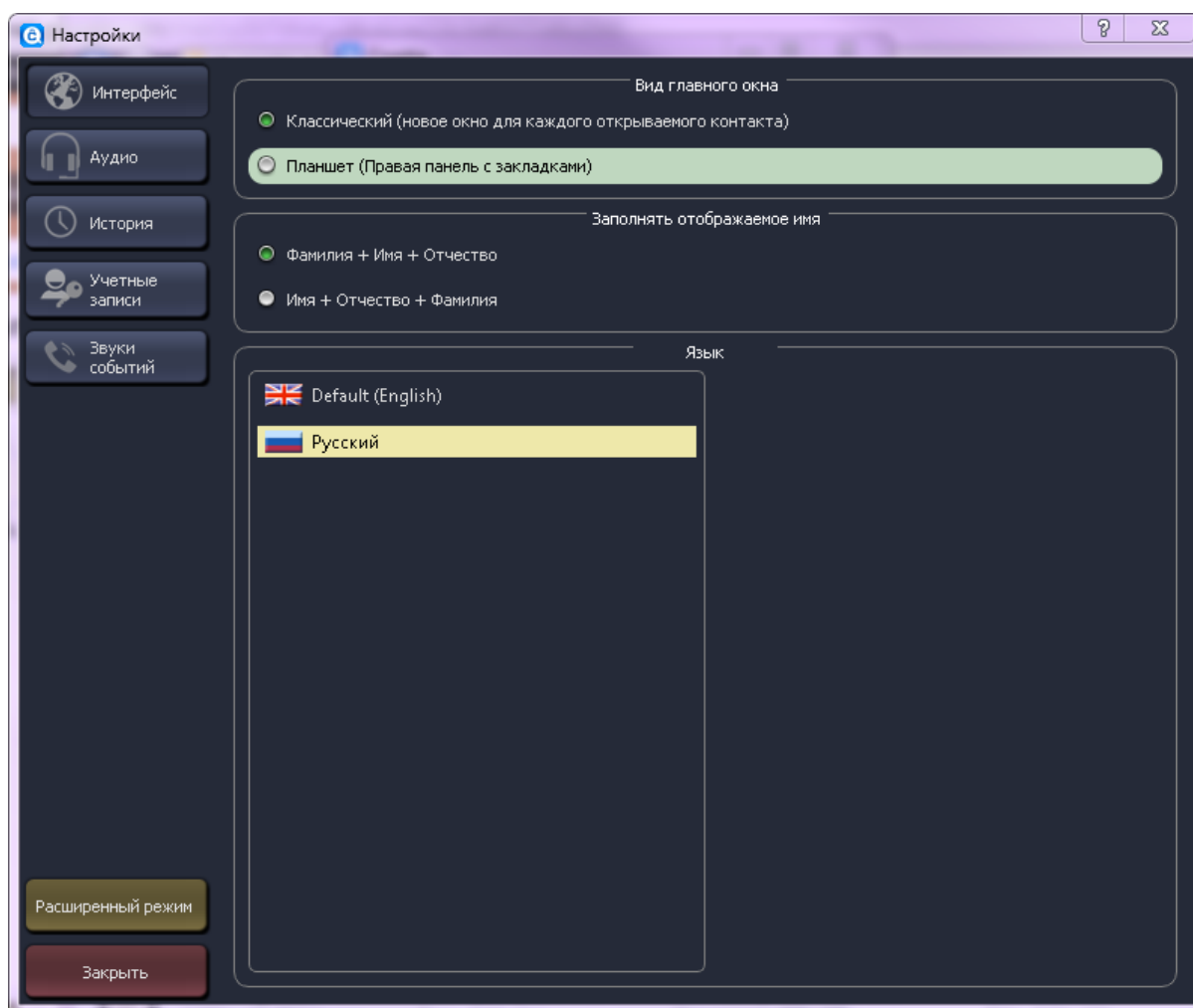


После того, как вы успешно зарегистрировали учетную запись, перед вами откроется главное окно программы. Его элементы подробно рассмотрены в [соответствующем разделе](#) данного Руководства. Сейчас просто нажмите на кнопку *Меню* в левом верхнем углу и выберите пункт *Настройки*.



4.2 Настройка языка

Первое, что вам может понадобиться в настройках — возможность смены языка программы. По умолчанию программа запустится на том языке, на котором происходила её установка. Если вас это не устраивает, обратитесь к первой вкладке окна настроек — *Интерфейс*.

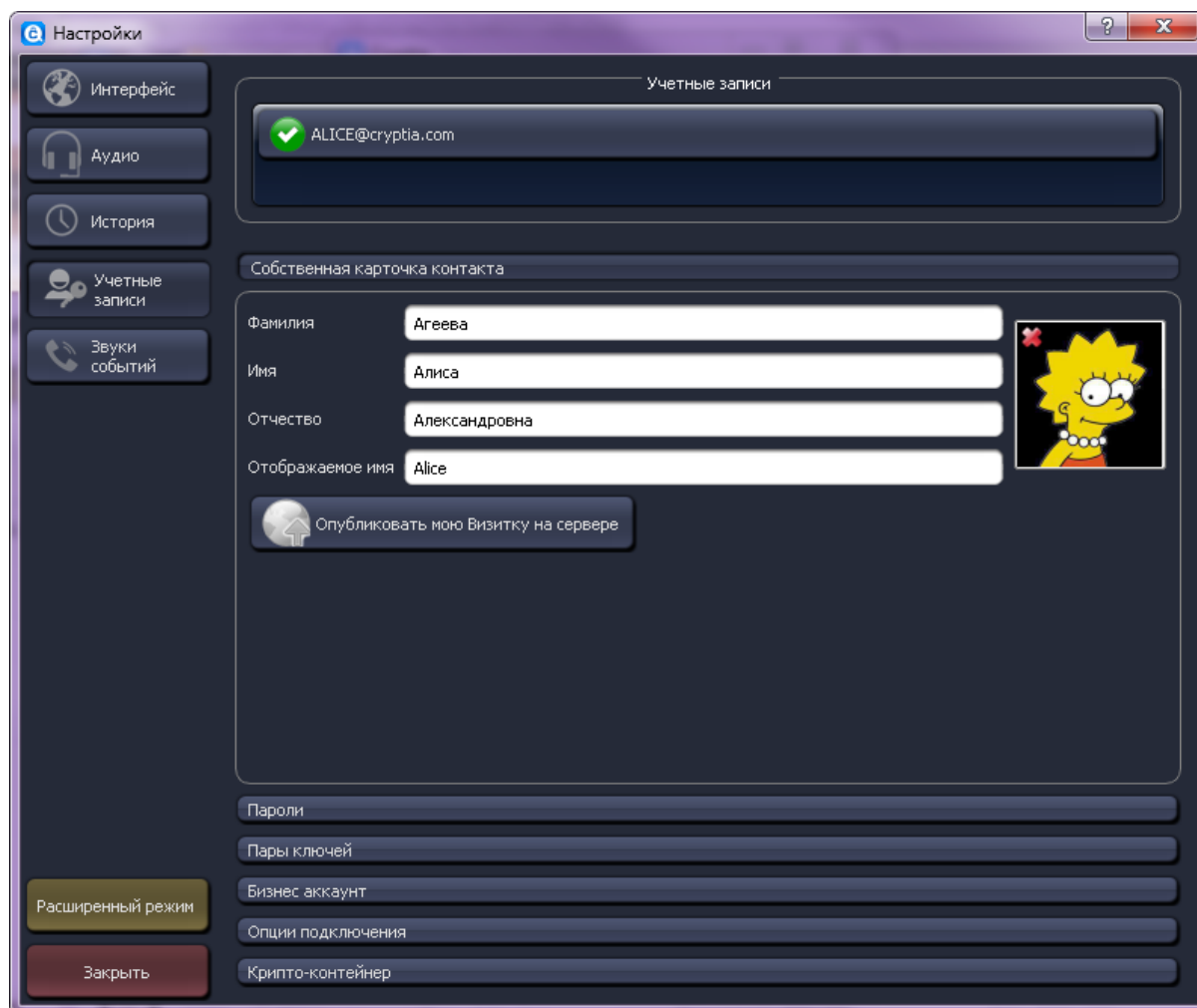


В центральной части окна находится список поддерживаемых языков. Если нынешний язык программы вам непонятен, ищите знакомый флаг.

Больше информации о параметрах, настраиваемых во вкладке Интерфейс, вы найдете [здесь](#).

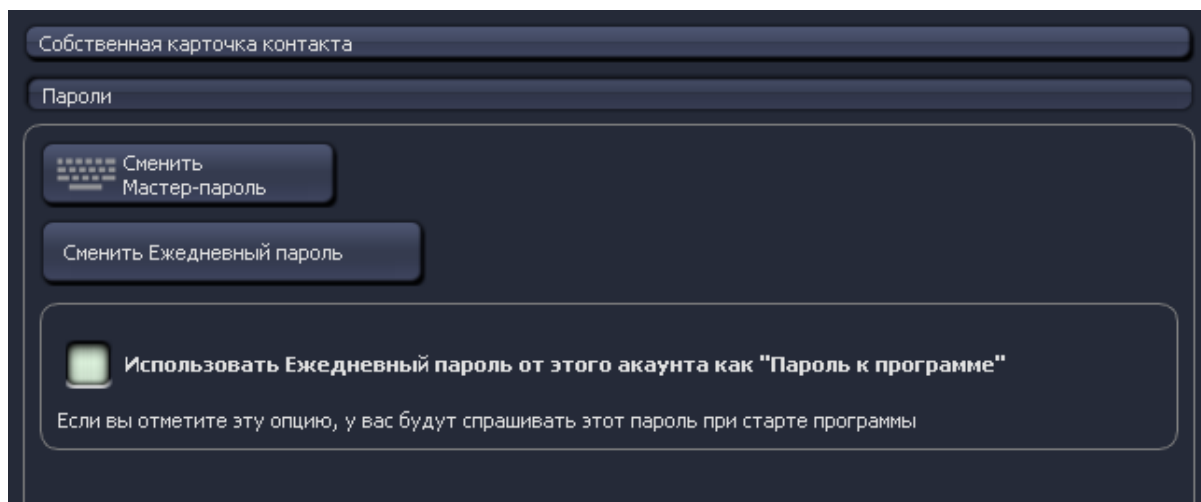
4.3 Редактирование визитки и смена паролей

Обратите внимание на вкладки, расположенные в левом верхнем углу окна *Настройки*. Нажмите на вкладку *Учетные записи*. Окно *Настройки* примет следующий вид:



Как видите, редактировать визитку для учетной записи очень просто. Внесите данные в соответствующие поля и, при желании, добавьте вашу фотографию, щелкнув на схематичном портрете справа – введенные данные сохраняются автоматически. Как уже было сказано выше, опция *Опубликовать визитку на сервере* определяет, будут ли пользователи, нашедшие ваш логин с помощью поиска, видеть вашу визитку. Если вы хотите удалить уже опубликованную визитку с сервера, очистите все поля и еще раз нажмите *Опубликовать визитку на сервере* — сервер перестанет хранить любую информацию о вас.

Обратите внимание на пять дополнительных кнопок под визитной карточкой. Это — **разделы** вкладки *Учетные записи*, более подробно мы их рассмотрим далее. А пока выберите раздел *Пароли*, щелкнув на соответствующую кнопку.



Здесь содержатся кнопки, позволяющие сменить пароли. Естественно, при смене пароля необходимо указать уже существующий. Функция галочки *"Использовать пароль от этого аккаунта как пароль к программе"*, расположенной ниже, понятна из ее описания - если эта галочка отмечена, при каждом старте Сcryptia вам необходимо вводить ежедневный пароль от этой учетной записи.

4.4 Подключение дополнительных учетных записей

Мы находимся во вкладке *Учетные записи* окна *Настройки*. Знаете ли вы, что программа имеет дополнительные возможности для работы с учетными записями, помимо показанных в этом окне? Нажмите кнопку *Расширенный режим* в левом нижнем углу.

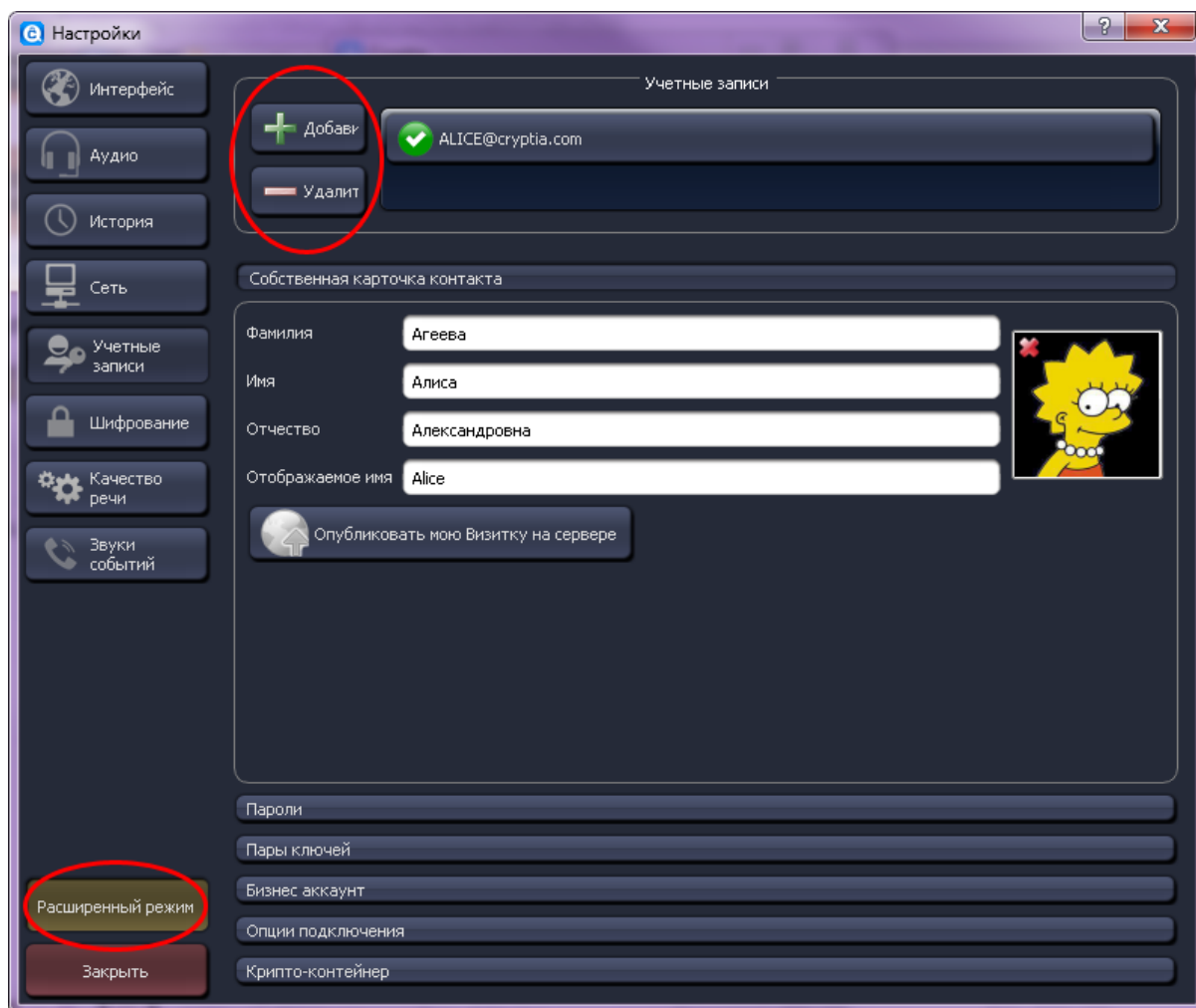
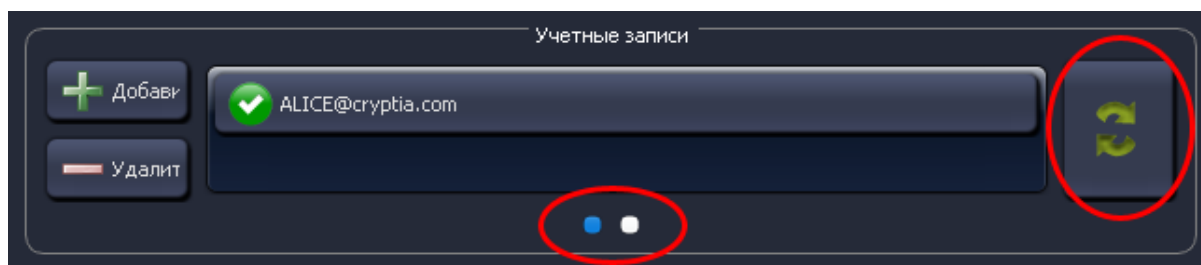


Рисунок выше демонстрирует, что в зоне вверху окна, рядом со строкой статуса подключения появились новые кнопки: **+Добавить** и **-Удалить**. Они служат для подключения новых учетных записей и для удаления с этого устройства уже существующих.

Нажмите на **+Добавить** и вы увидите уже знакомое окно *Настройка учетной записи*. В нем вы можете [зарегистрировать новую](#) учетную запись, или подключить к этому компьютеру [уже зарегистрированную](#). Таким образом, как уже было сказано, вы можете использовать как одну учетную запись на разных компьютерах, так и несколько учетных записей на одном компьютере.

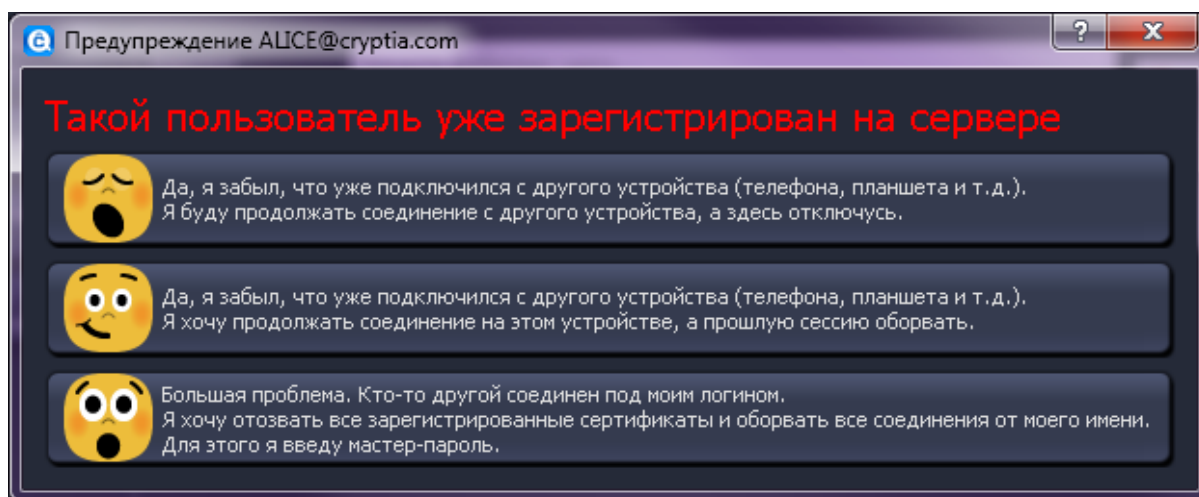


Как только вы подключите еще одну учетную запись, появляются новые кнопки. Кнопка справа от строки статуса служит для последовательного переключения между зарегистрированными на этом устройстве учетными записями. Настройки применяются только для выбранной на данный момент

записи. Обратите внимание также на точки под строкой статуса — каждая точка соответствует одной учетной записи, и нажатие на точку перенесет к настройкам соответствующей учетной записи. Эти же точки присутствуют в *Главном окне* Cryptia.

Для того чтобы удалить учетную запись с этого компьютера, нажмите кнопку *-Удалить*. Это действие очистит всю историю общения под удаляемой учетной записью, а также список контактов. Так как сервер Cryptia не хранит подобную информацию, удаление учетной записи необратимо. Подключив удаленную учетную запись к компьютеру еще раз, вы не сможете восстановить никакую информацию, удаленную ранее вместе с этой записью.

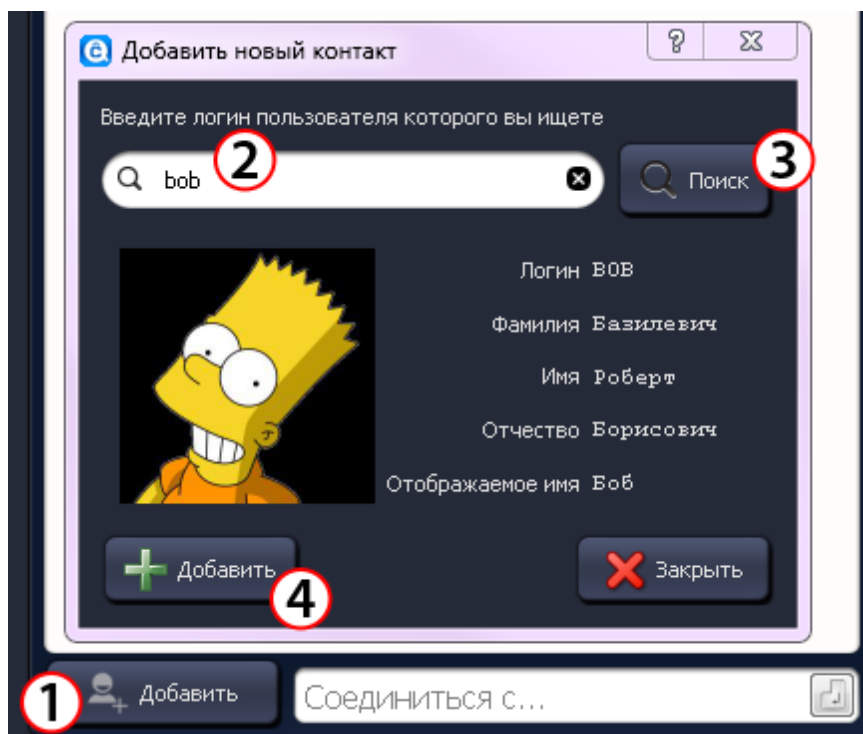
Примечание: Один клиент может быть подключен к нескольким учетным записям, но одна учетная запись не может быть открыта в двух клиентах одновременно. Если вы попытаетесь подключиться к учетной записи, к которой уже совершено подключение, вы увидите следующее окно, опции которого интуитивно понятны:



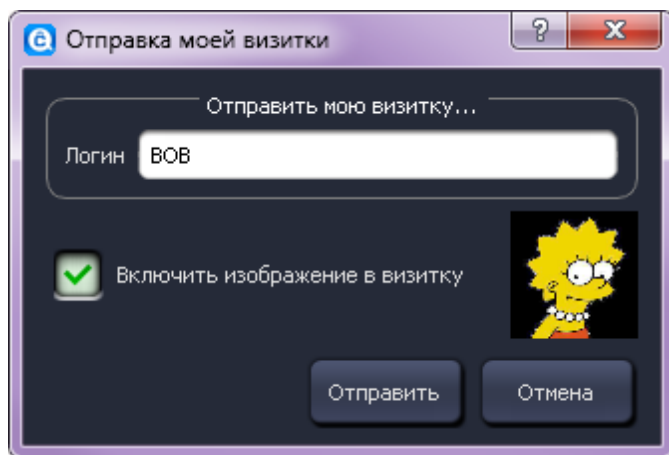
5 Быстрый старт: начинаем общение

5.1 Добавление контакта

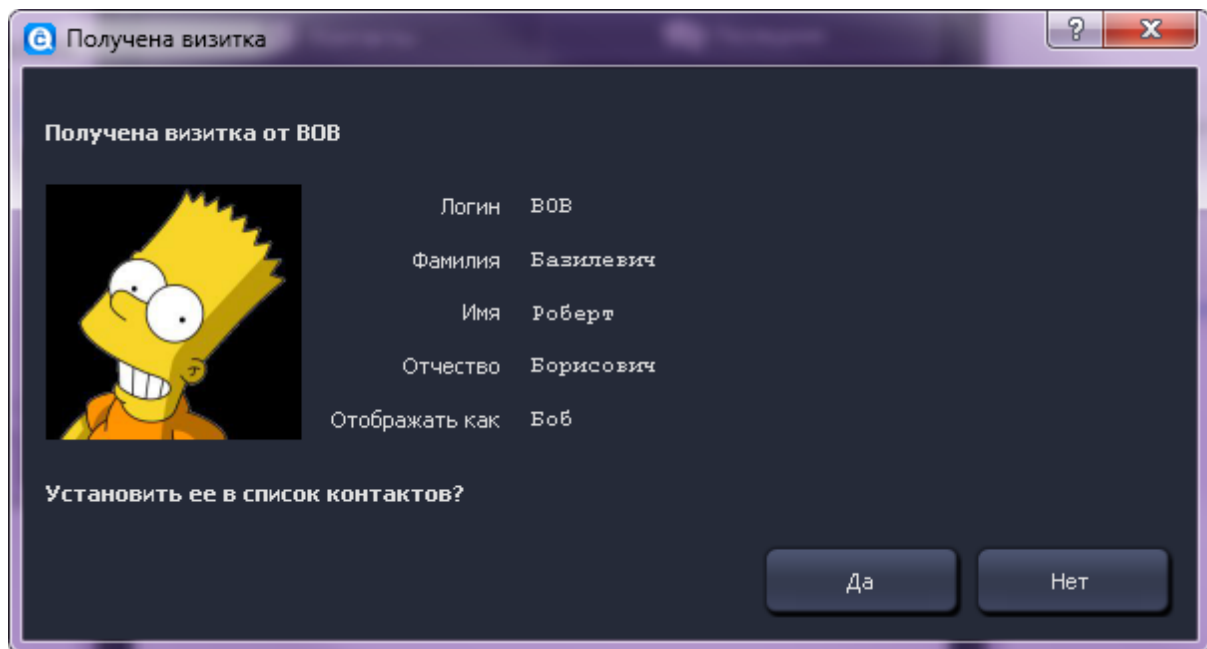
Для того чтобы общаться с помощью Cryptia, необходимо установить соединение с целевым абонентом. Для установки такого соединения нужно, чтобы у вас была визитка этого абонента (и желательно, чтобы этот абонент располагал вашей). Поэтому процесс добавления контакта связан с обменом визитками.



Вернемся к главному окну программы. Нажмите на кнопку *Добавить контакт* (1) в левом нижнем углу программы. В появившемся окне введите логин целевого абонента (2) и нажмите кнопку *Поиск* (3). **Если абонент опубликовал свою визитку на сервере**, то вы увидите ее в этом же окне. Нажмите *Добавить* (4), чтобы сохранить эту информацию в своем списке контактов.



Сразу после этого программа предложит вам отправить свою визитку этому абоненту. Если абонент находится в сети, он получит запрос и сможет подтвердить свое желание общаться с вами.



Если эти условия были соблюдены, и абонент находится онлайн, его запись в списке контактов будет выглядеть следующим образом:

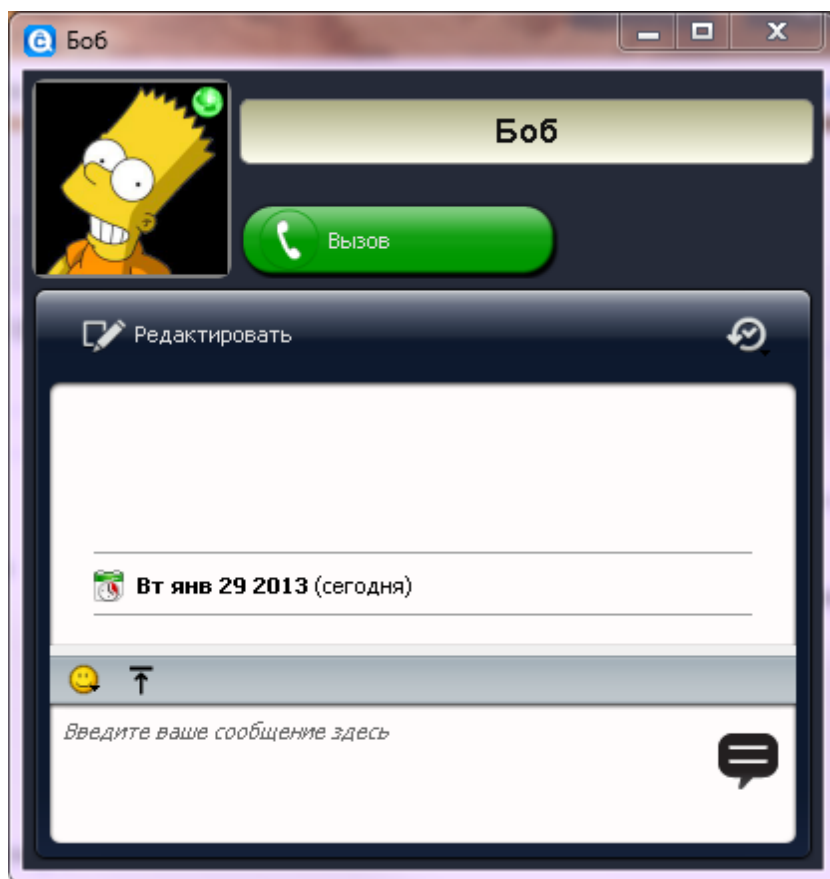


Обратите внимание на зеленый индикатор справа от схематичного портрета. Он означает, что вы можете начинать общение. Если индикатор серый, поговорить не удастся.

Примечание: существует возможность обмениваться визитками минуя сервер, [экспортировав визитку в файл](#) и передав этот файл каким-либо другим способом.

5.2 Общение

Дважды нажмите на контакт в списке контактов. Откроется окно соединения.



Зеленый индикатор в правом верхнем углу портрета означает, что пользователь находится онлайн. Для общения с помощью Cryptia необходимо, чтобы оба собеседника находились в сети, так как соединение устанавливается напрямую, и никакие промежуточные серверы в нем не участвуют.

Как только вы напишете текстовое сообщение, отправите файл или нажмете кнопку голосового вызова, соединение начнет устанавливаться. Обладая **бизнес-акаунтом**, вы можете устанавливать неограниченное число таких соединений; бесплатный абонент с одной учетной записи может за день установить соединение только с пятью другими бесплатными абонентами (каждый день эти пять абонентов могут быть другими; ограничений на общение с бизнес-абонентами нет).

Введите текстовое сообщение в поле внизу окна — и увидите, как в окне соединения появится дополнительная информация:



Особое внимание уделите **контрольному коду** — он служит индикатором того, что конфиденциальность соединения не нарушена. Вы можете сверить контрольные коды с вашим собеседником — то, что они совпадают, означает, что никакое третье лицо не наблюдает ваш разговор.

Соединение прервется, как только вы или ваш собеседник закроете это окно. Если вы захотите продолжить разговор, потребуется установить соединение заново.

В процессе общения вы располагаете такими опциями — **текстовые сообщения, голосовой вызов и пересылка файлов**. Первый способ мы уже рассмотрели; для начала голосовой связи служит зеленая кнопка *Голосовой вызов* вверху окна соединения. Теперь посмотрите на панель вверху поля для ввода текста:

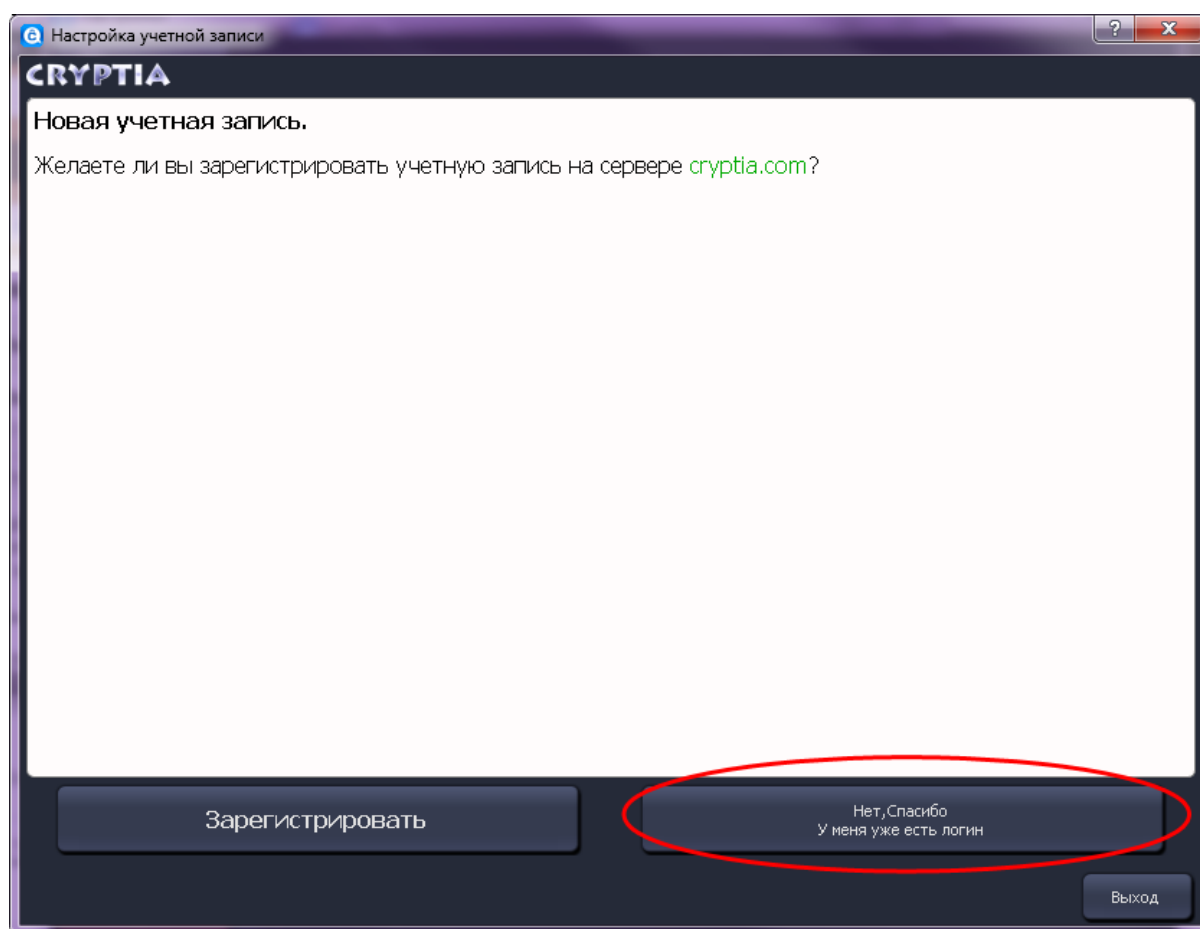


Первая кнопка позволяет вам разбавить ваши текстовые сообщения анимированными смайликами. Вторая кнопка этой панели вызывает стандартное для операционной системы меню, в

котором вы можете выбрать файл для пересылки абоненту. Точно так же другие абоненты могут пересылать файлы вам. Полученные вами таким образом файлы будут сохранены в [криптоконтейнер](#), если он подключен. Если вы не используете криптоконтейнер, файлы сохраняются в папку, [предварительно назначенную](#) во вкладке *Интерфейс* окна *Настройки*. Убедитесь, что на криптоконтейнере достаточно свободного места или что у вас есть права записи в желаемую папку.

6 Работа с учетными записями

6.1 Подключение учетной записи. Учетные записи, созданные на другом сервере.



Если [в окне](#) *Настройка учетной записи* нажать кнопку *Нет, спасибо, у меня уже есть логин*, программа предоставит возможность подключить к программе учетную запись, созданную на другом компьютере. Процесс подключения учетной записи практически не отличается от создания новой. Вам необходимо вспомнить мастер пароль к вашей учетной записи и указать ежедневный пароль (помните, что ежедневный пароль может отличаться от ежедневных паролей к этой учетной записи на других устройствах).

Настройка учетной записи

CRYPTIA

Настройка для имеющейся учетной записи.

Укажите ваш логин на сервере cryptia.com.

Надеемся, вы помните ваш мастер-пароль.

Ежедневный пароль необязательный. Вы можете оставить его пустым. Если он указан, вам придется вводить его каждый раз при регистрации на сервере.

Этим паролем шифруется ваш список контактов, история ваших сообщений, криптоконтейнер с полученными файлами и приватные ключи.

Ежедневный пароль не передается на сервер, а используется для шифрования файлов на вашем устройстве.

Если у вас имеется учетная запись на другом сервере поставьте отметку напротив "Другой сервер" и укажите адрес сервера.

☐ Другой сервер

Логин Максимум 20 символов. Только латинские символы цифры и символы "." и "_"

Мастер-пароль

Ежедневный пароль

Повторите Ежедневный пароль

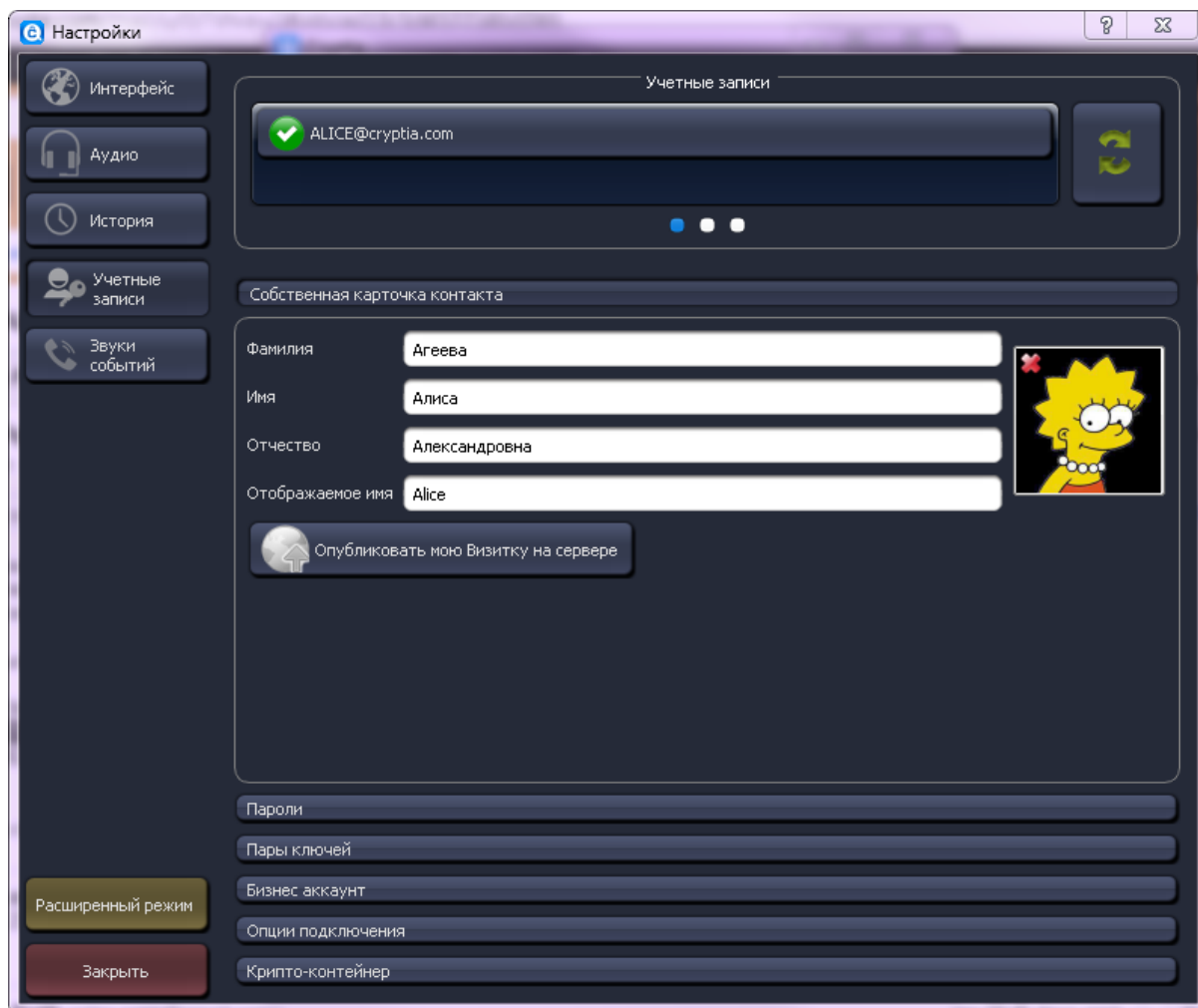
Назад Далее Выход

Если подключаемая запись расположена на сервере cryptia.com (т. е. была создана вами непосредственно в программе Cryptia), нажмите *Далее*>. Если вы хотите подключить запись, созданную на каком-либо другом сервере, отметьте галочку *Другой сервер* и укажите его адрес в появившемся ниже поле.

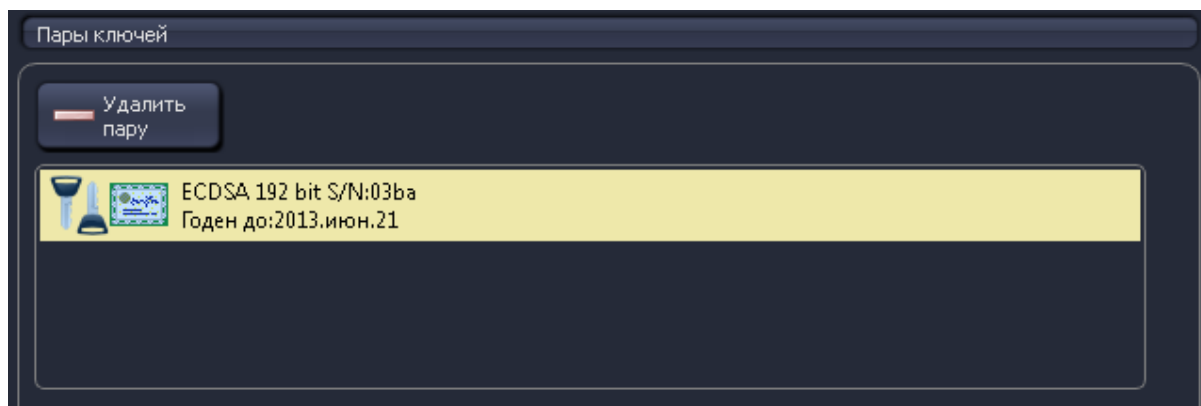
☒ Другой сервер

Адрес сервера

6.2 Пары ключей



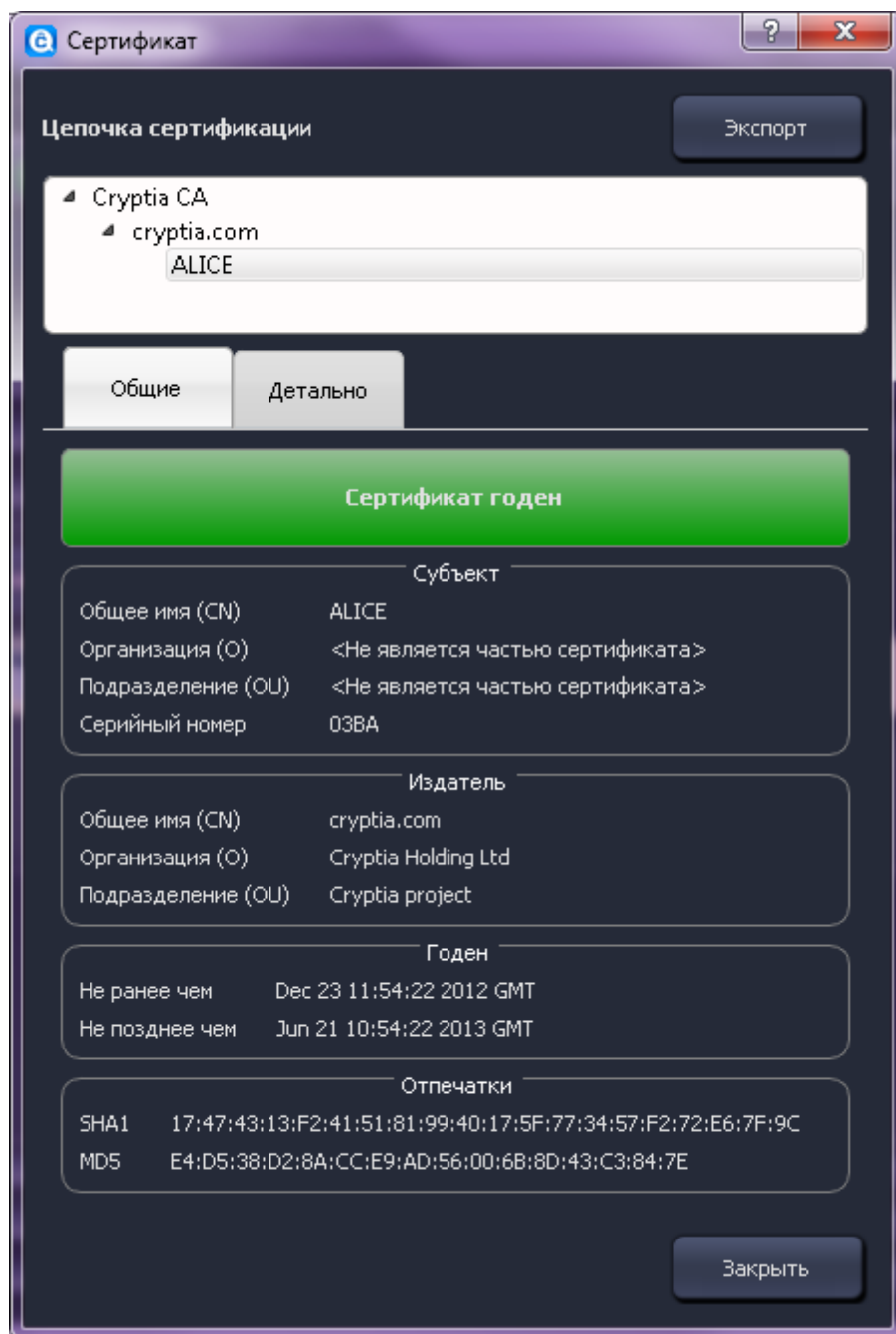
На рисунке выше изображено окно *Настройки*, вкладка *Учетные записи*. Помимо инструментов добавления, удаления и переключения между учетными записями, [рассмотренных в Быстром Старте](#), эта вкладка содержит шесть разделов. Первые два также [описаны в Быстром Старте](#), работа с ключами будет рассмотрена в этом параграфе, а три оставшиеся — в следующих.



Пара ключей — это то, что используется для подтверждения подлинности установленного соединения — с сервером, или с другим пользователем. **Публичный ключ** — это та часть ключевой пары, которую получает адресат соединения, и с ее помощью он может проверить подлинность сообщений. Приватный ключ - хранится на компьютере (устройстве) владельца ключа и никогда и никуда не передается. С помощью приватного ключа можно подписать сообщения, проверить подлинность которых может любой обладатель публичного ключа. Обладатель публичного ключа не имеет возможности подписать сообщение. Технология использования ключевых пар является краеугольным камнем всей криптографии.

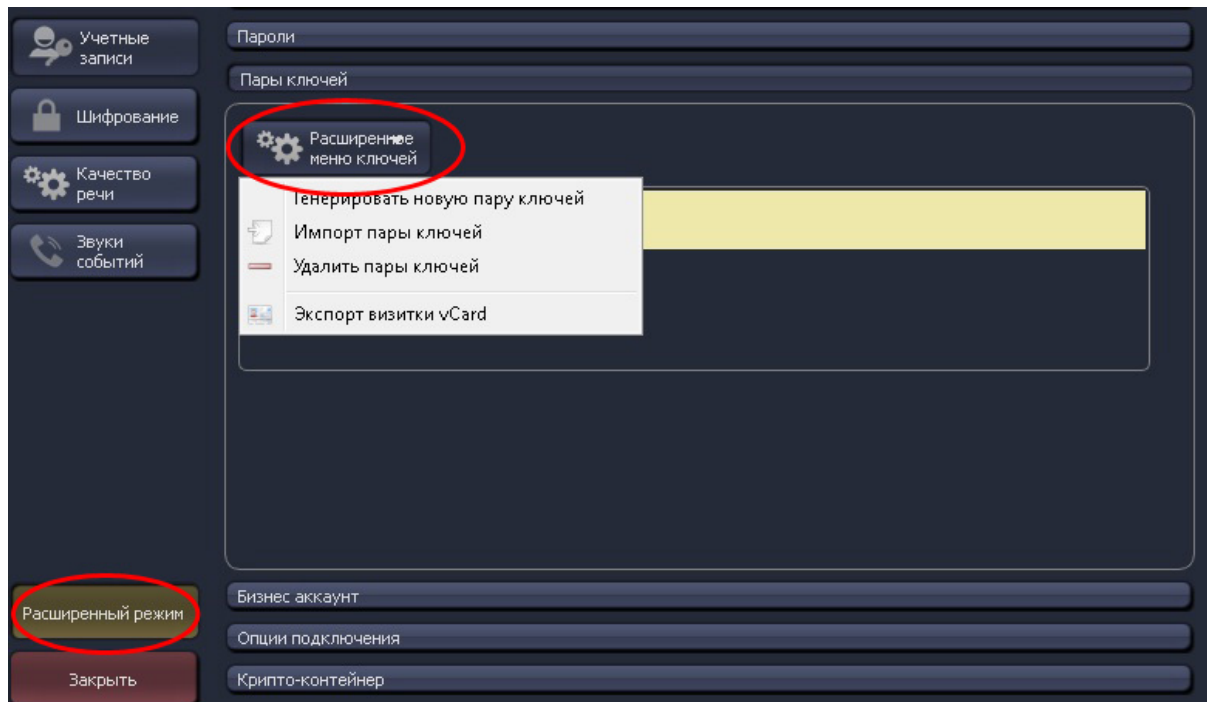
Для каждой учетной записи на каждом компьютере сервер создает минимум одну уникальную пару ключей, устанавливающую подключение к серверу. Ваш приватный ключ от этой пары шифруется с помощью [ежедневного пароля](#), если он есть.

Сертификат — это, по сути, публичный ключ с заложённой в него информацией о владельце. Эта информация подтверждает подлинность самого публичного ключа. Дважды нажмите на пару ключей, чтобы посмотреть общую информацию о сертификате.



В разделе *Пары ключей* вкладки *Учетные записи* можно просмотреть сертификаты для всех имеющихся пар ключей. Пиктограмма возле этой пары ключей показывает статус сертификата. Вот таблица возможных статусов:

	Новая пара ключей сгенерирована, но сертификат (как подтверждение подлинности) еще не получен.
	Пара ключей с действующим сертификатом
	Пара ключей с отозванным сертификатом. Ее нельзя использовать, можно только удалить. Об отзыве сертификатов см. параграф «Отзыв сертификатов и режим «Невидимка» следующего раздела данного Руководства.
	Запрос на получение сертификата отвергнут сервером сертификации. Этого не произойдет в случае если вы формировали запрос при помощи программы Cryptia или при помощи OpenSSL. В случае если вы импортировали поврежденный сертификат, или сертификат с алгоритмом публичного ключа, который нам не известен, такое возможно.
	Отправлен запрос на отзыв сертификата, но процесс отзыва не завершен. Программа не будет использовать такие пары ключей, однако удалить ее еще нельзя до завершения процесса отзыва.

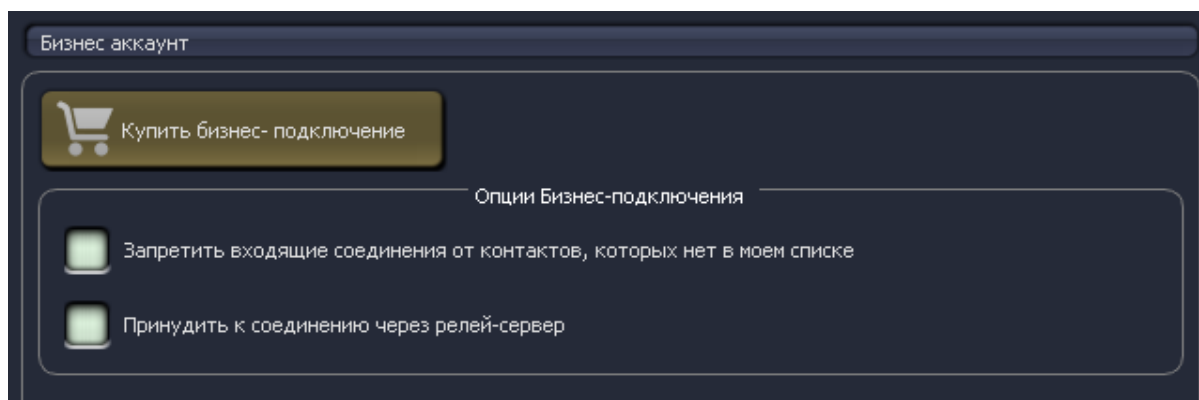


Если включен *Расширенный режим*, то над списком сертификатов во вкладке *Пары ключей* расположено *Расширенное меню ключей*. С его помощью вы можете создать новую пару ключей, используя нужный вам алгоритм, импортировать или удалить пару ключей. Еще одна опция — *экспортировать визитку в файле vCard*. При этом у вас есть возможность добавить к визитке любые сертификаты, которые сочтете нужными. Пользователи, получив от вас файл, будут [импортировать вашу визитку](#) и/или сертификаты с помощью *Редактирования контакта*.

Создание нового ключа позволит вам указать алгоритм - RSA, DSA или ECDSA, и его параметры, такие как длину ключа или эллиптическую кривую соответственно. Этот процесс может занять от нескольких секунд до нескольких десятков минут. После завершения генерации пары ключей будет сохранен приватный ключ (в зашифрованном виде, если присутствует ежедневный пароль) и

сформирован файл запроса сертификата с публичным ключом. Если вы соединены с сервером, то Вам будет предложено сразу отправить этот запрос на сервер для получения сертификата — но вы сможете, при желании, отправить этот запрос позднее.

6.3 Бизнес-подключение



Как уже было сказано выше, бесплатные пользователи Cryptia ограничены в количестве других бесплатных пользователей, с которыми они могут совершить подключение — пять в день. Но подключения к пользователю, обладающему бизнес аккаунтом, не входят в этот лимит. Естественно, бизнес-подключение снимает все подобные ограничения.

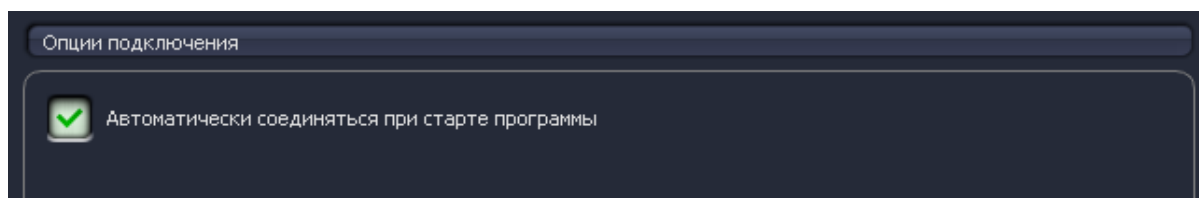
Для того, чтобы совершить одноразовое подключение (см. строка одноразового подключения внизу [Главного окна программы](#)), один из собеседников должен иметь бизнес-подключение. Если вы обладаете бизнес-подключением, и не желаете, чтобы другие пользователи имели возможность связаться с вами подобным образом, отметьте галочку *Запретить входящие соединения от контактов, которых нет в моем списке*.

Принудительное соединение через релей (транзитный) сервер означает, что ваш трафик при прямых соединениях будет обязательно пропущен через транзитный сервер, даже если это не требуется для установки прямого соединения. Ваш собеседник не будет видеть ваш IP адрес, а вместо этого будет видеть IP адрес релей-сервера. Если он также использует эту опцию, трафик будет идти через два релей-сервера.

Трафик может пропускаться через релей-сервер также в отдельных случаях, если невозможно установить прямое соединение между абонентами. По умолчанию основной сервер выделит вам подходящий релей исходя из своих соображений, когда в этом возникнет потребность, или когда отмечена соответствующая галочка.

Нажатие на кнопку *Купить бизнес-подключение* откроет веб-страницу в вашем браузере, в которой вы сможете совершить покупку.

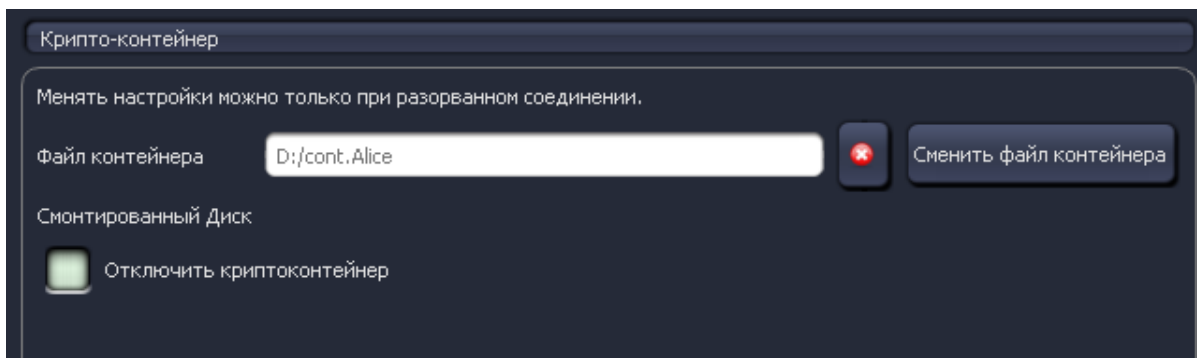
6.4 Автоматическое соединение с сервером



Раздел *Опции подключения* вкладки *Учетные записи* содержит только одну опцию.

Автоматическое подключение учетной записи к серверу при старте программы возможно лишь в том случае, если пара ключей не зашифрована, то есть если ежедневный пароль не установлен.

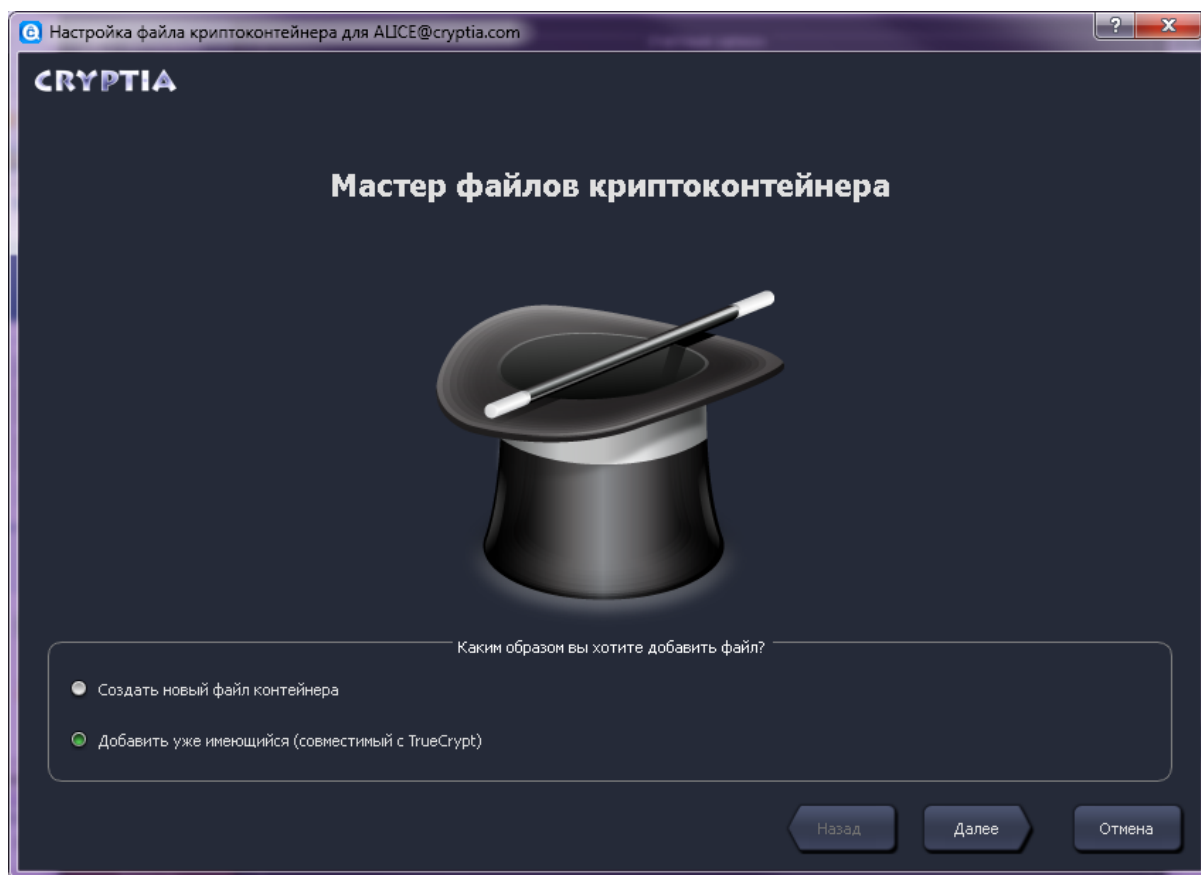
6.5 Расширенная работа с криптоконтейнером



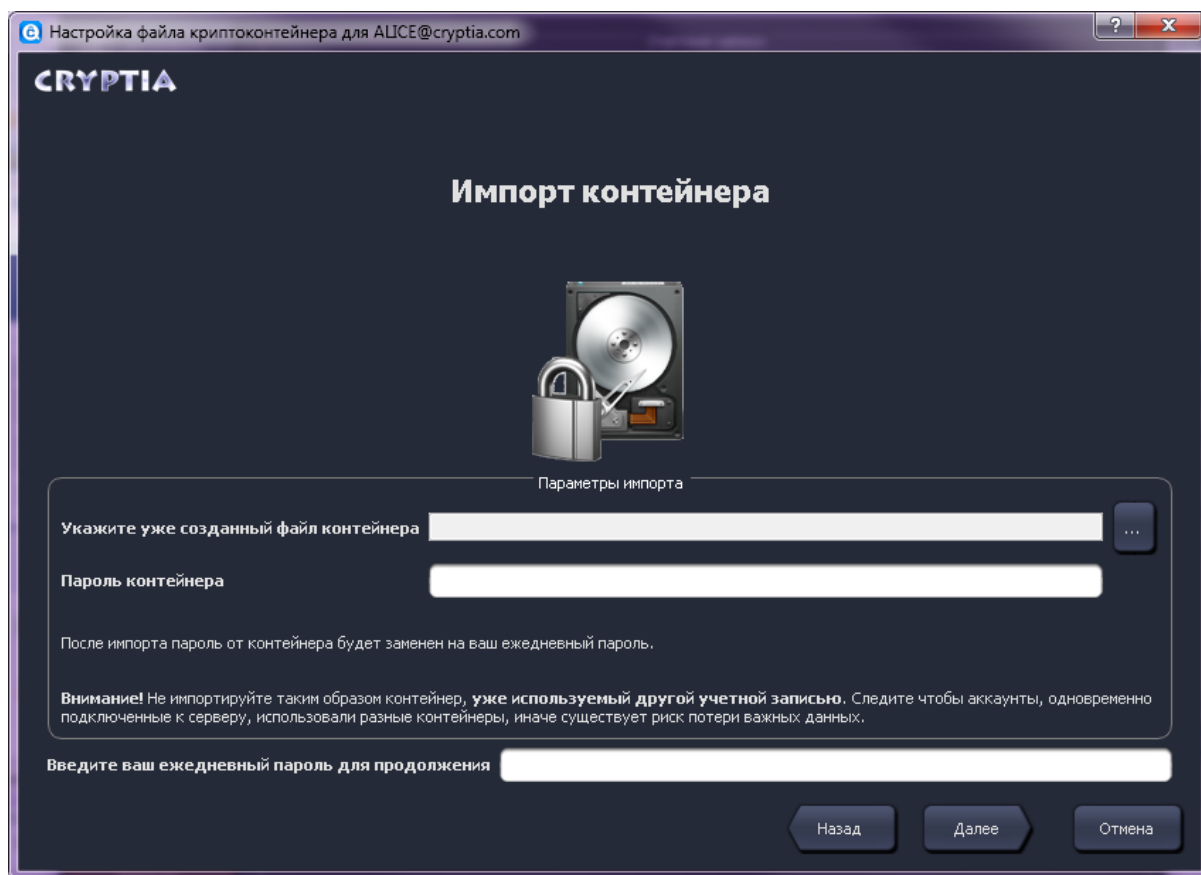
Настройки вкладки *Криптоконтейнер* возможно изменить лишь в случае, **если ваша учетная запись не подключена к серверу.**

Под строкой пути к файлу находится индикатор, показывающий букву смонтированного виртуального диска (для Windows). Расположенные справа от строки кнопки позволяют отключить файл контейнера или подключить новый. После отключения контейнера файл остается в том же месте - если вы хотите его удалить, вам предстоит это сделать вручную. Галочка *Отключить криптоконтейнер* позволяет временно приостановить использование криптоконтейнера, с возможностью продолжить без переподключения.

Кнопка изменить файл контейнера вызовет следующее окно:



Первая опция - создать новый файл - приведет вас к [уже знакомому](#) окну создания криптоконтейнера. Если вы выберете "подключить существующий файл", откроется следующее окно:



Вам следует указать путь к уже существующему файлу контейнера и пароль к нему. Если вы создавали контейнер с помощью TrueCrypt, пароль следует вводить в треугольных скобках. Скажем, если при создании вы указали пароль вида *Мой_Пароль*, то в этом окне нужно ввести *<Мой_Пароль>*. Хотя мы надеемся, конечно, что вы выбрали пароль понадежнее. Если вы создавали контейнер с помощью Cryptia, в поле *Пароль к контейнеру* следует ввести ежедневный пароль к учетной записи, для которой этот контейнер создавался.

И в первом, и во втором случае, пароль от этого контейнера будет изменен на ежедневный пароль текущей учетной записи (то есть той, к которой вы подключаете контейнер). Ежедневный пароль от текущей учетной записи следует ввести в соответствующее поле в самом низу окна.

Ни в коем случае не подключайте контейнер к двум учетным записям одновременно! Отсоедините файл контейнера от других учетных записей Cryptia, прежде чем подключать, иначе вы рискуете невозможной потерей данных.

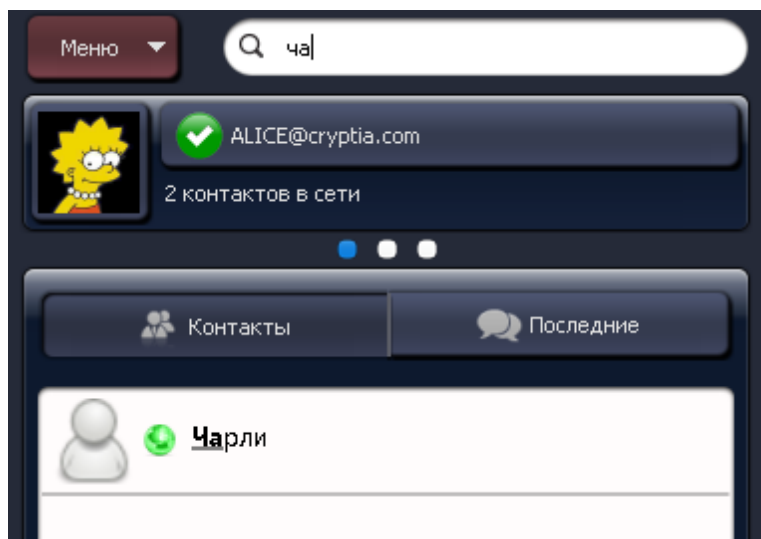
7 Главное окно, список контактов и история

7.1 Элементы главного окна программы



- 1) Кнопка вызова меню программы, в котором доступны *Настройки*, *Журнал сообщений* и окно *О программе*. В последнем можно узнать номер текущей версии Cryptia.
- 2, 4) Иконка-индикатор и строка состояния подключения (см. [следующий раздел](#)).
- 3) Строка фильтрации списка контактов. В списке контактов отображаются учетные записи, отображаемые имена которых соответствуют заданному в этой строке критерию поиска. На практике это означает, что если вы введете в строку последовательность символов, список контактов отобразит только контакты, включающие в себя эту последовательность (см. рис. ниже). Вы можете переключать учетные записи с помощью точек-индикаторов (6), при этом строка

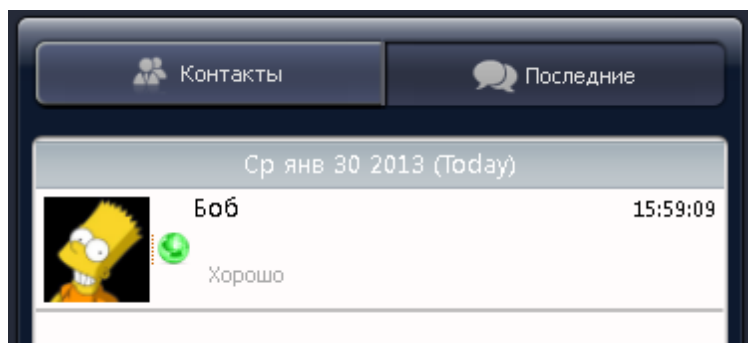
фильтрации не будет сбрасываться.



5) Ваш портрет, как он задан в визитке. Нажатие на него откроет вкладку *Учетные записи* окна *Настройки*.

6) Индикаторы учетных записей. Вы можете подключить сколько угодно учетных записей к одной программе. Каждой подключенной записи отвечает одна точка. Нажимайте на точки, чтобы переключаться между учетными записями. Для каждой учетной записи необходимо совершать подключение к серверу отдельно.

7) Переключатель между **списком контактов** и **списком разговоров**. Если вы нажмете кнопку *Последние*, вместо контактов список будет отображать ваши последние разговоры:



8) Список контактов. Дважды нажмите на контакт, чтобы вызвать [окно соединения](#) с контактом.

Нажмите правой кнопкой на контакте, чтобы вызвать [контекстное меню](#), позволяющее удалить или отредактировать информацию об этом контакте.

9) Кнопка [Добавить контакт](#).

10) Строка ввода логина для одноразового соединения без обмена визитками и без добавления в список контактов. Доступна только для [бизнес-подключения](#) — то есть пользователи с бизнес-подключением могут связаться с помощью этой функции с любым другим пользователем (зная его логин), бесплатные пользователи могут одноразово связаться столько с бизнес-пользователями.

7.2 Статус соединения



В самом верху Главного окна (а также вкладки Учетные записи окна Настройки) расположена строка состояния подключения. Нажатие на нее прервет соединение с сервером (или инициирует процедуру логина в случае, если учетная запись к серверу не подключена). Для того чтобы сразу узнать о состоянии подключения посмотрите на иконку слева. Возможные варианты:



Подключение в порядке



Ошибка подключения



В процессе подключения

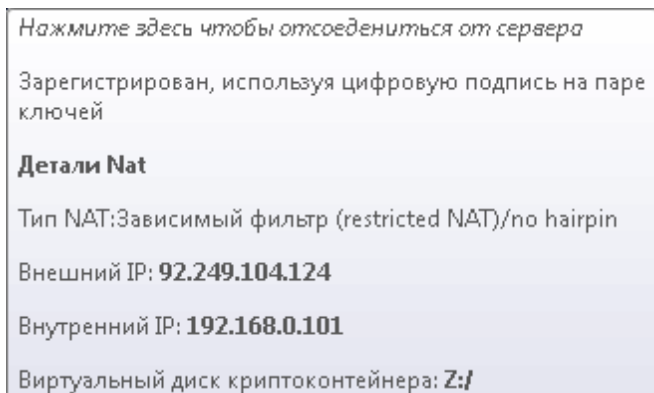


Отключено пользователем

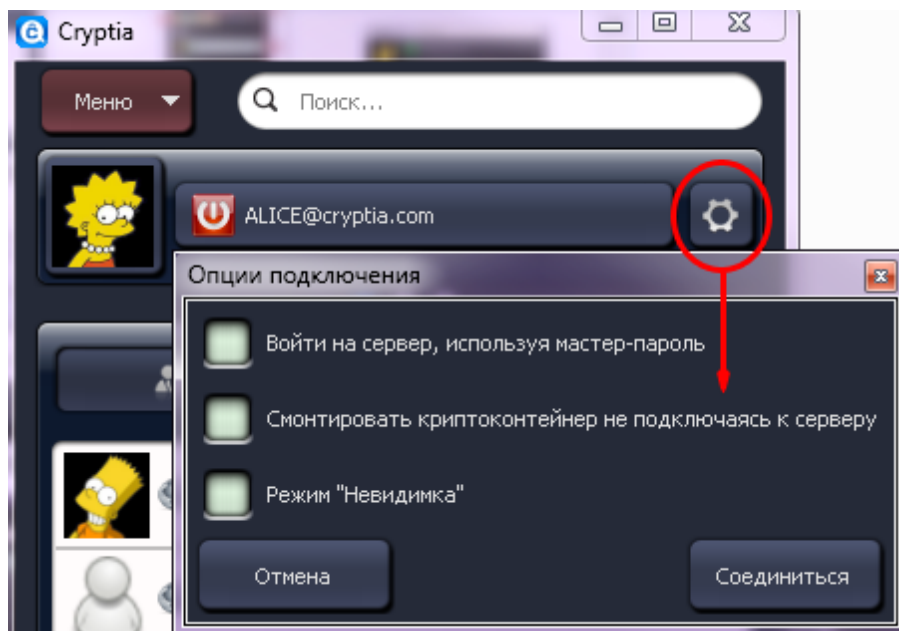


Подключен криптоконтейнер, соединения с сервером нет.

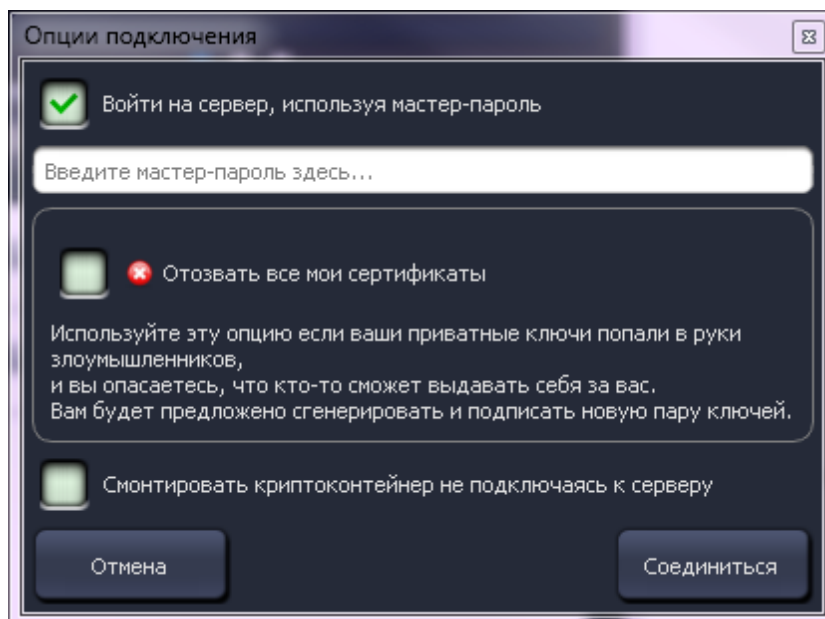
Кроме того, если вы несколько секунд задержите указатель мыши на строке состояния, то увидите всплывающую подсказку с дополнительной информацией.



7.3 Отзыв сертификатов и режим "невидимка"



Нажмите на строку статуса подключения, чтобы отключить текущее подключение к серверу. Рядом со строкой статуса появится кнопка с изображением шестеренки (см. рис. выше), нажатие на которую откроет окно Текущие опции подключения. Эта кнопка появляется также, если установить соединение с сервером не удалось по какой-либо причине.



Вход на сервер с помощью мастер-пароля может быть полезным в многих случаях. Особенно нужно им воспользоваться, **если кто-либо завладел вашим приватным ключом**, и имеет возможность заходить в вашу учетную запись с его помощью. В таком случае отметьте галочку *Отозвать все мои сертификаты* после ввода мастер-пароля. После того, как соединение будет установлено, все пары ключей к этой учетной записи потеряют свою силу и их нужно будет

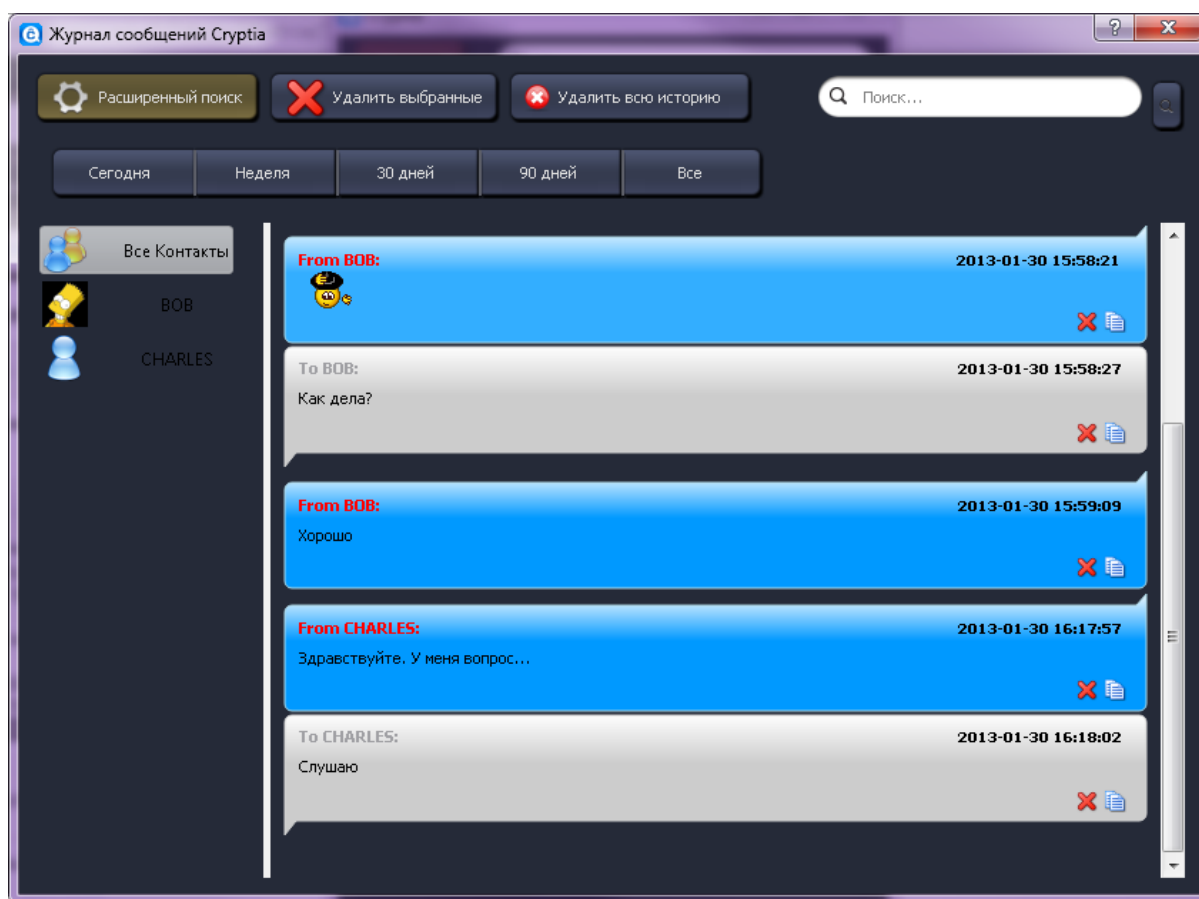
создавать заново. Имейте в виду, что зайдя при помощи мастер-пароля, нельзя инициировать и принимать звонки. В этом режиме можно только работать с парами ключей и/или менять пароль.

Режим «Невидимка» определяет, будут ли другие пользователи, в списке контактов которых вы находитесь, видеть — онлайн вы или нет.

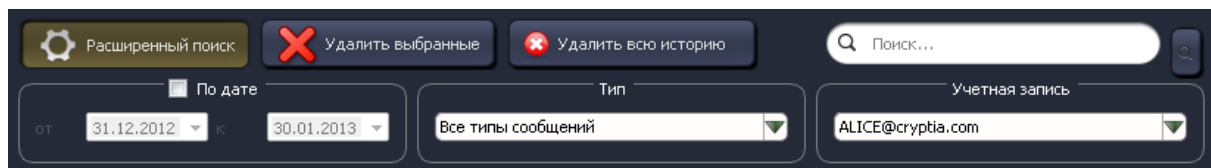
Также с помощью этого инструмента у вас есть возможность смонтировать криптоконтейнер не подключаясь к серверу.

7.4 Журнал сообщений

Меню программы, находящееся в левом верхнем углу Главного окна Cryptia, помимо доступа к *Настройкам*, позволяет открыть *Журнал сообщений*. В журнале сообщений записываются: входящие и исходящие текстовые сообщения, сообщения об ошибках и другая информация от сервера, отправленные и полученные файлы. Естественно, голосовые разговоры в журнале не записываются.

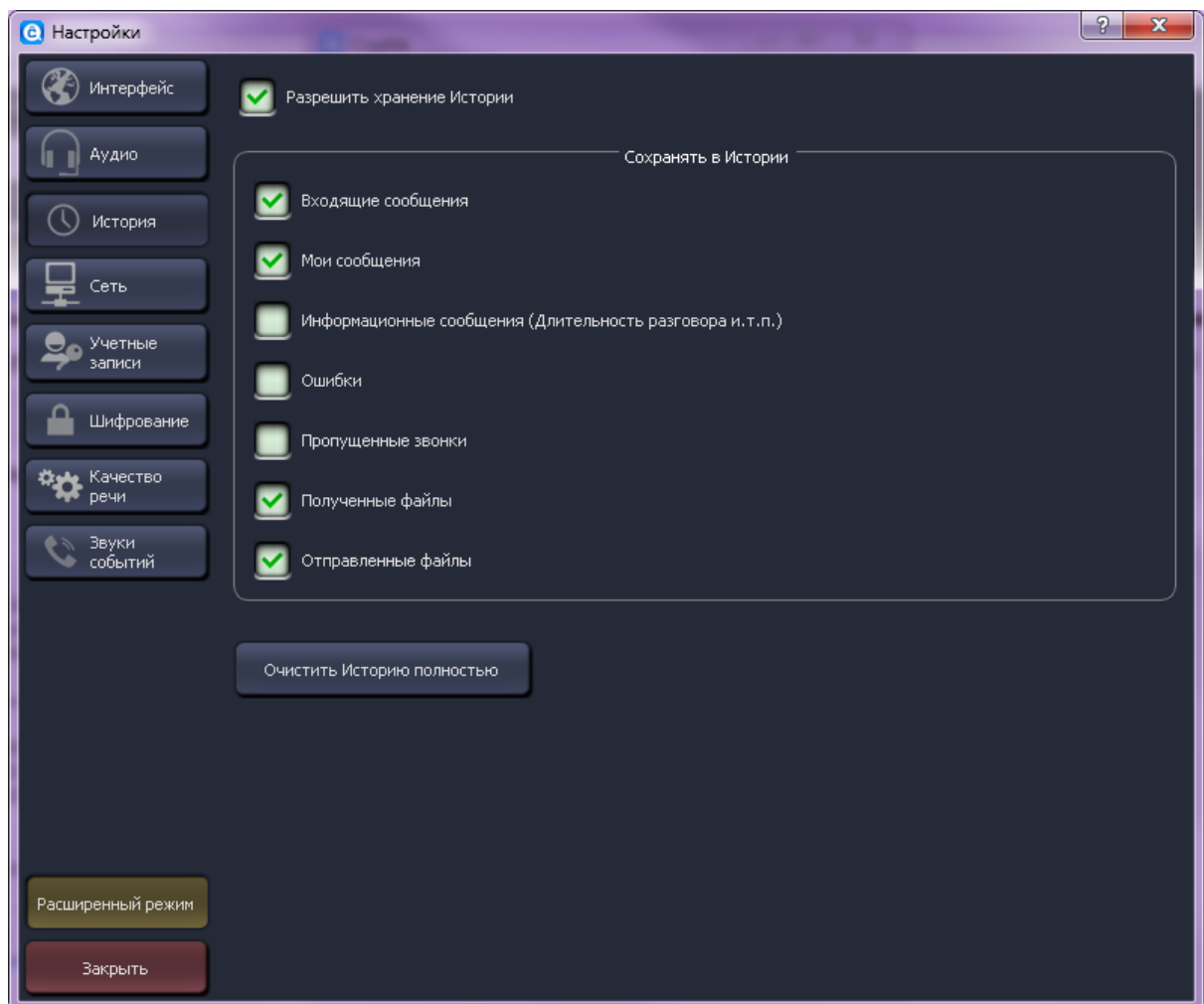


Данное окно может похвастаться интуитивным интерфейсом. В центральной области расположены просматриваемые сообщения, каждое из которых можно удалить или скопировать в буфер обмена с помощью соответствующих кнопок. С помощью кнопок с именами собеседников в левой части окна вы сможете фильтровать разговоры, состоявшиеся с разными контактами. Выше находятся дополнительные опции фильтрации, такие как поиск по конкретной фразе или по дате.



Нажав на *Расширенный поиск*, вы можете более точно указать диапазон дат фильтруемых сообщений, а также их тип (текстовые сообщения, файлы, информационные сообщения и др.). Имейте в виду, что журнал истории хранит разговоры, совершенные от имени всех учетных записей, подключенных к этому компьютеру, "вперемешку". Выпадающий список *Учетная запись* в опциях *Расширенного поиска* позволяет отфильтровать разговоры, состоявшие от имени какой-либо конкретной учетной записи.

7.5 Настройки - вкладка История



Эта вкладка окна *Настройки* при включенном *Расширенном режиме* позволяет указать, сообщения какого типа будут сохраняться в журнале событий. Кнопка *Очистить Историю полностью* делает именно то, что на ней написано.

7.6 Редактирование данных о контакте

Вернитесь к главному окну программы. При нажатии правой кнопкой мыши на контакт в списке контактов появится контекстное меню для этого контакта:



Три опции, расположенные внизу, рассмотрены в разделе Быстрый старт: начинаем общение (ссылка). Удаление пользователя из списка контактов приведет к тому, что на вашем компьютере не будет храниться никаких данных об этом пользователе, включая историю сообщений между вами и этим пользователем. Для того чтобы возобновить общение с этим пользователем, необходимо повторно добавить его контакт — но удаленная история сообщений восстановлена не будет.

Окно Редактирование контакта позволяет изменить информацию об этом контакте. Поле Отображать как отвечает за то, как пользователь будет виден в вашем списке контактов. Вы можете назначить Рингтон данного контакта (то есть звук, с помощью которого программа сообщает о попытке этого пользователя связаться с вами), указав путь к файлу формата .mp3 или .wav в соответствующем поле. При нажатии на кнопку Дополнительно окно Редактирование контакта примет следующий вид:

Редактирование контакта

Логин: BOB

Сохранить

Фамилия: Базилевич

Отмена

Имя: Роберт

Импорт из vCard

Отчество: Борисович

Отображать как: Боб

Дополнительно

Рингтон

Режим "Невидимка" для этого контакта

Экспорт в vCard

Сертификаты

Добавить

Удалить

Просмотр

Кеш параметров алгоритмов согласования ключа

Алгоритм: Диффи-Хеллман на эллиптических кривых - 256 бит

Хэш: 6c7e0a6be40bbc9414f88f5010919929

Помещен: 30.01.2013 Последнее использование: 30.01.2013Использ...

Добавить

Удалить

В дополнительных настройках вы можете видеть принадлежащие данному контакту [сертификаты](#) и [параметры алгоритмов согласования ключа](#), если такие хранятся.

Сертификаты, которые используются при установке защищенного соединения именно с этим контактом, могут быть переданы в визитной карточке или же установлены отдельно. Нажатие на кнопку **Добавить** в группе **Сертификаты**, чтобы занести сертификат вручную. Если сертификат присутствует, его можно посмотреть, нажав на кнопку **Просмотр**. Обратите внимание, что если при просмотре сертификата не установлено подключение к серверу, то верификация сертификата не будет работать.

Парметры алгоритма согласования сеансового ключа ([Диффи-Хеллман](#) или Диффи-Хеллман на эллиптических кривых), передаются от инициатора разговора к принимающей стороне при установлении первого контакта. Далее программа сохраняет эти параметры в кеш для последующих подключений. Эти параметры передаются публично, то есть через сервер — хотя это и не несет в себе почти никакой угрозы вашей безопасности, есть возможность вручную занести набор этих параметров в кеш, в случае чего эти параметры вообще никогда не будут

передаваться в открытом виде.

Функции импорта и экспорта файлов vCard раскрыты [в следующем разделе](#).

7.7 Обмен визитными карточками без участия сервера

Если ваш предполагаемый собеседник решил [не публиковать свою визитную карточку на сервере](#), то вы не сможете получить с сервера никакой информации о нем, кроме его логина. Этот пользователь может передать вам визитку при добавлении контакта, а может передать вам файл формата vCard, чтобы вы его импортировали, и получили из него информацию и присоединенные сертификаты. Для этого воспользуйтесь кнопкой *Импорт из vCard* в окне *Редактирование контакта* (см. [предыдущий раздел](#)). Здесь же вы можете создать файл формата vCard, содержащий информацию о вашем контакте, для передачи третьим лицам.

Редактирование контакта

Логин: BOB

Фамилия: Базилевич

Имя: Роберт

Отчество: Борисович

Отображать как: Боб

Рингтон: [Выбор файла]

Сохранить

Отмена

Импорт из vCard

Дополнительно

Экспорт в vCard

Режим "Невидимка" для этого контакта

Сертификаты

Добавить

Удалить

Просмотр

Кеш параметров алгоритмов согласования ключа

Алгоритм: Диффи-Хеллман на эллиптических кривых - 256 бит

Хэш: 6с7е0а6be40bbs9414f88f5010919929

Помещен: 30.01.2013 Последнее использование: 30.01.2013Использ...

Добавить

Удалить

Для того чтобы экспортировать собственную визитку в файл vCard, зайдите в *Настройки*, выберите

вкладку *Учетные записи*, раздел [Пары ключей](#). Кнопка *Расширенное меню ключей* содержит необходимые функции.

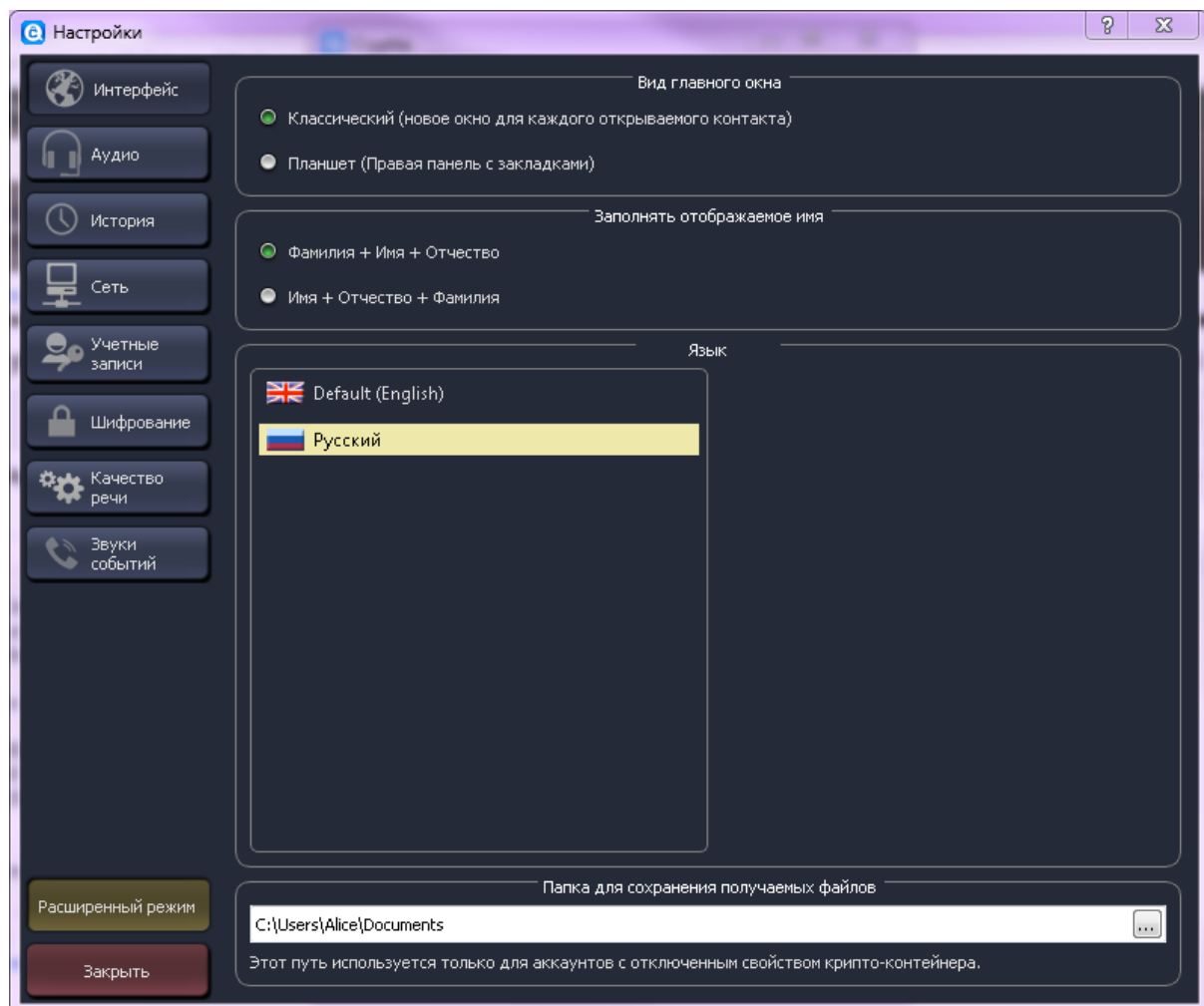
8 Настройки программы

8.1 Примечание к разделу

Этот раздел описывает все вкладки окна *Настройки*, кроме вкладки *Учетные записи*, описанной в [Быстром старте](#) и в разделе [Работа с учетными записями](#) и вкладки *История*, описанной в разделе, посвященном Журналу сообщений.

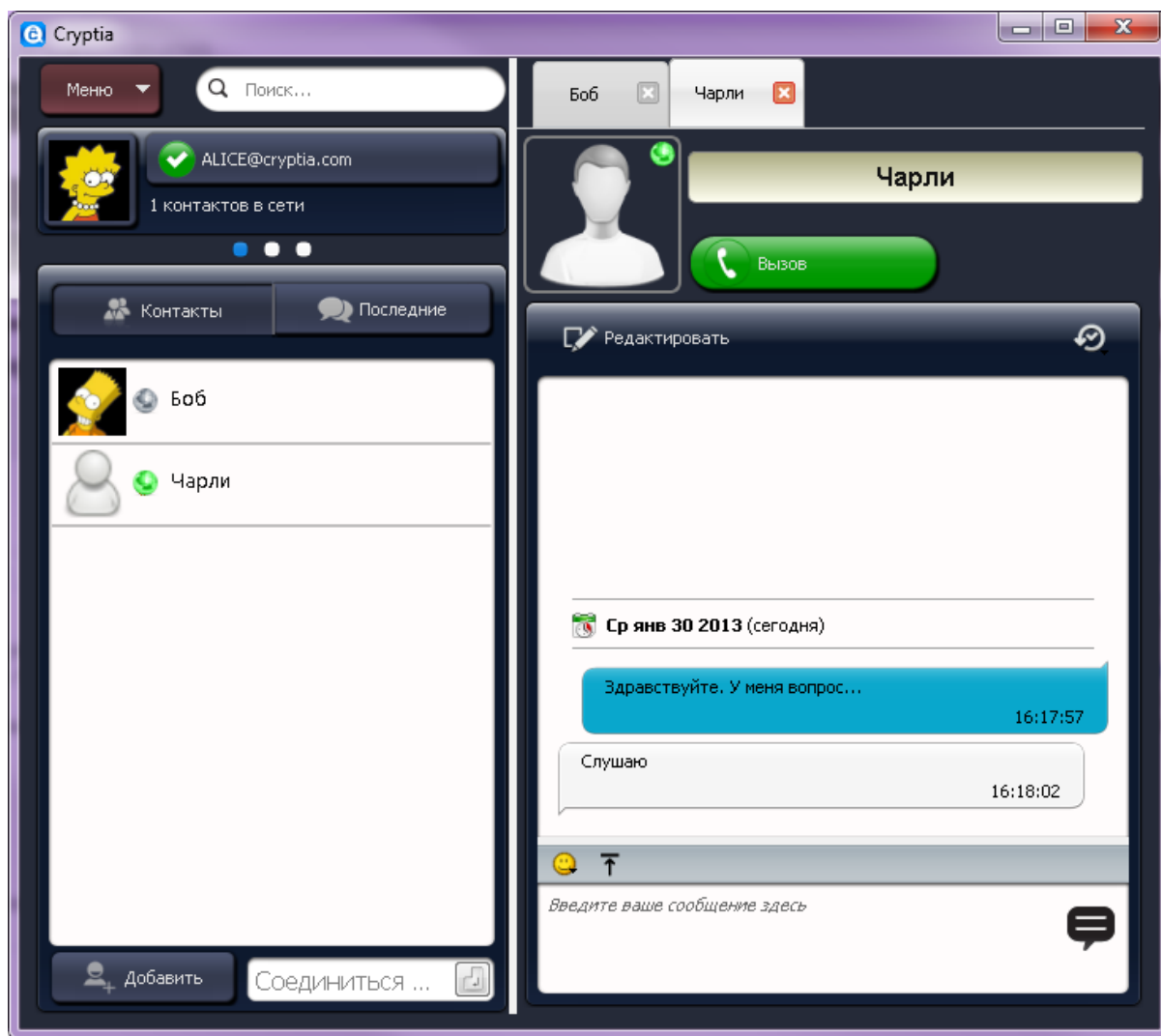
Если то или иное окно настроек на вашем экране не соответствует приведенному в руководстве изображению, убедитесь, что включен расширенный режим — вероятнее всего, кнопка или опция, которую вы не можете найти, относится к продвинутым настройкам. Учтите также, что внешний вид окна *Настройки* может незначительно отличаться от изображений данного руководства в зависимости от операционной системы, установленной на вашем компьютере.

8.2 Вкладка Интерфейс



Эта вкладка уже упоминалась в Быстром старте, в контексте [изменения языка программы](#). Дополнительно к рассмотренным по ссылке опциям вы можете указать ваши предпочтения по

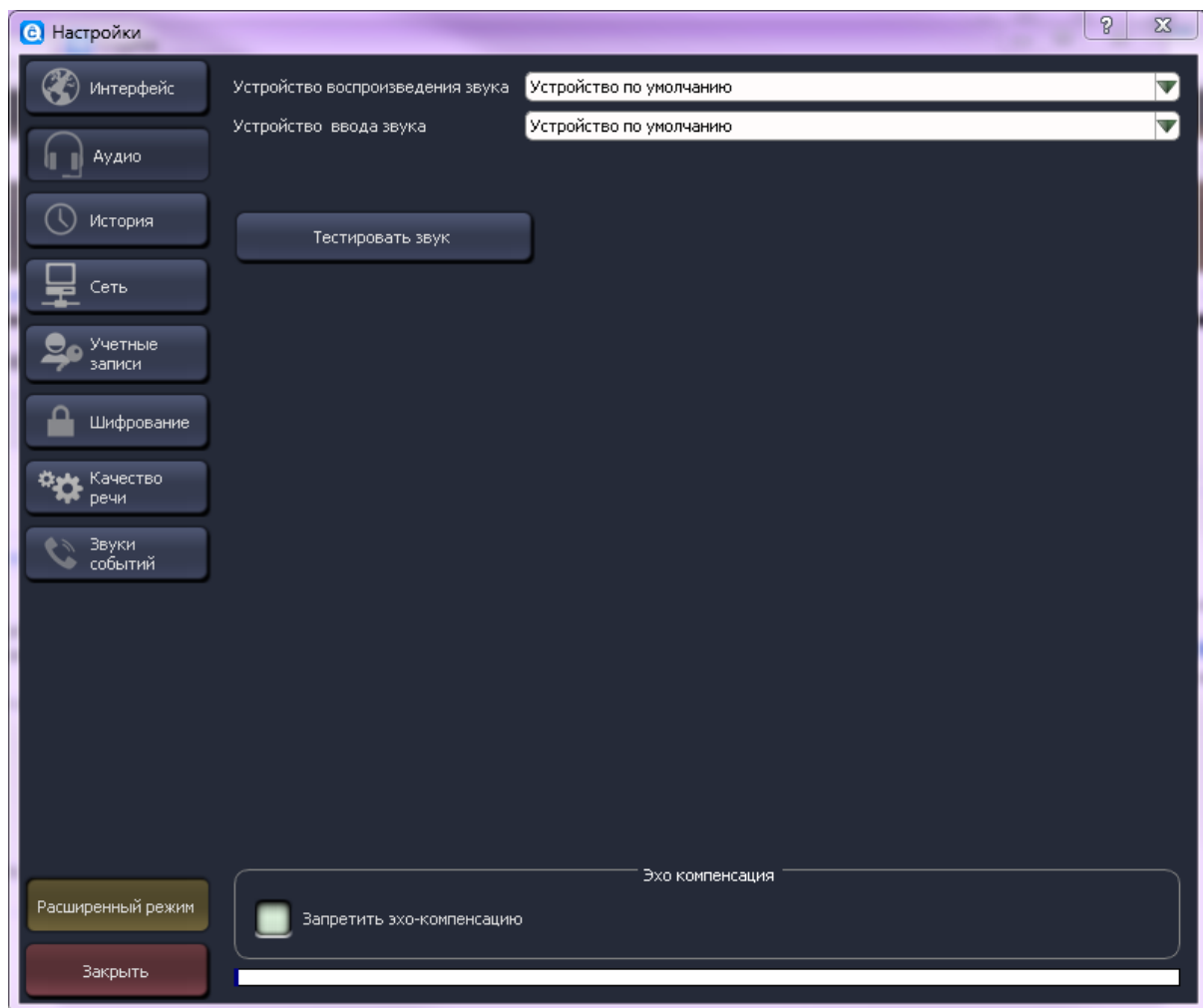
таким пунктам: *порядок отображения фамилии, имени и отчества* вашего собеседника из визитки в вашем списке контактов (если вы не указали другое **отображаемое имя**); *внешний вид программы*. Последний пункт определяет, будет ли каждый новый разговор открываться в отдельном окне, или главное окно вместе с разговорами будут помещаться в одном окне.



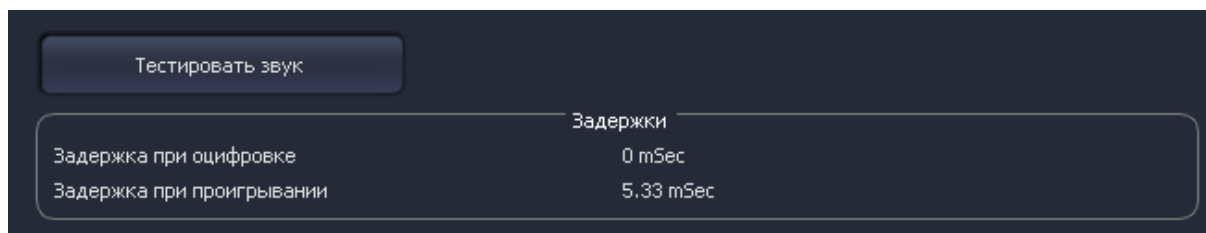
На рисунке выше изображена программа с настройками внешнего вида *Планшет*. Переключение между открытыми разговорами происходит с помощью вкладок справа вверху. Таким образом вам будет легче ориентироваться, если вы ведете одновременно несколько разговоров. К тому же, возможно, такой вид окажется для вас более привычным.

Расширенные настройки этой вкладки включают в себя *адрес папки*, куда будут сохраняться полученные файлы в случае отключения криптоконтейнера. Убедитесь, что у вас есть необходимые права доступа к этой папке для записи.

8.3 Вкладка Аудио

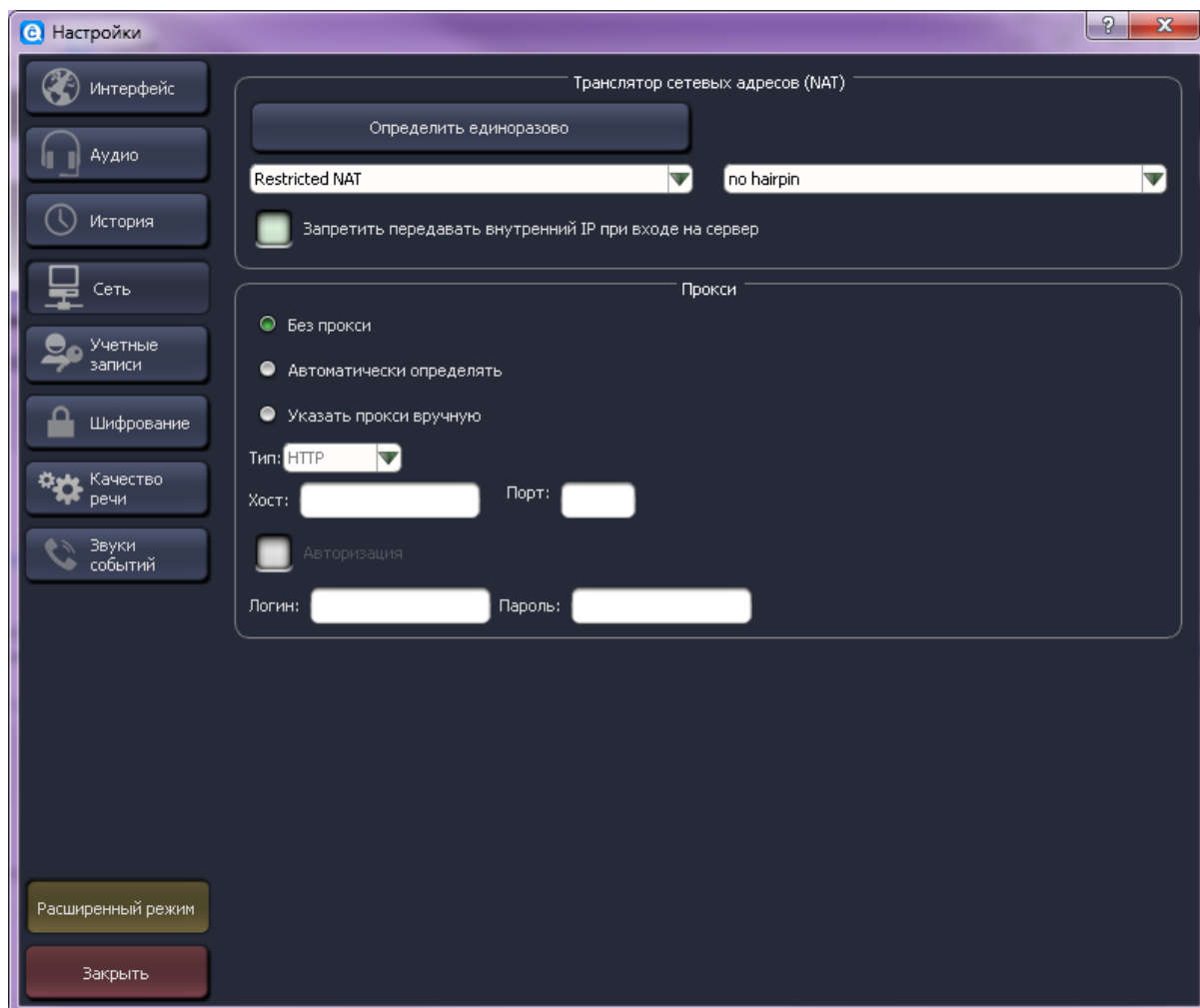


Если у вас несколько звуковых карт, здесь вы можете выбрать, какую именно будет использовать Cryptia. Также вы можете запретить *эхо-компенсацию*, если желаете сэкономить ресурсы компьютера. Если вы общаетесь через наушники или гарнитуру, в эхо-компенсации нет совершенно никакой необходимости.



Нажав на кнопку *Тестировать звук* вы запустите автоматический тест выбранной звуковой карты и увидите показатели задержки воспроизведения и записи.

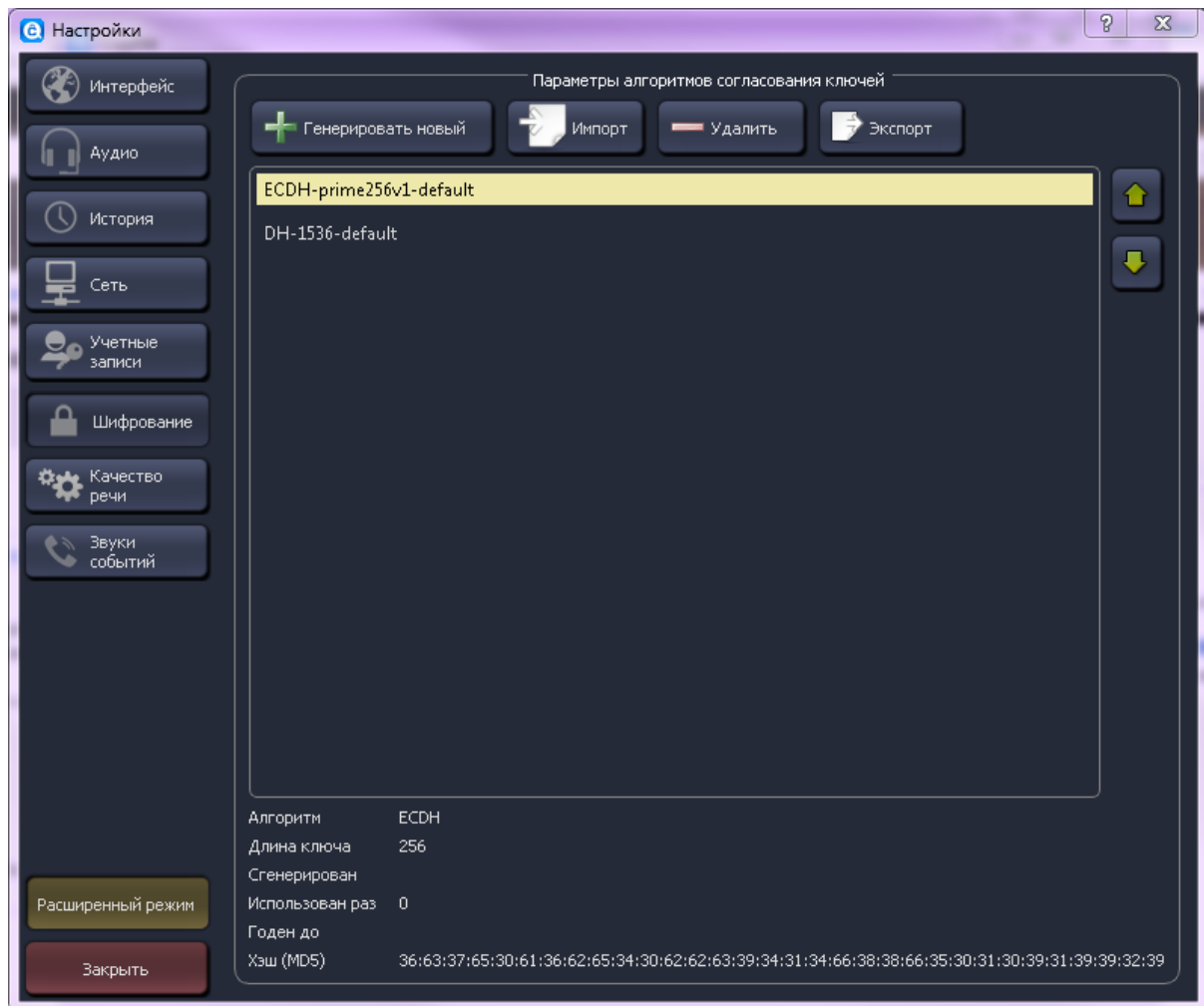
8.4 Вкладка Сеть — настройка подключения и NAT



Настройки сети доступны в *Расширенном режиме* и предназначены для экспертов. **NAT** ([Network Address Translation](#)) – это процесс маршрутизации трафика, то есть, например, используя роутер, вы используете этот механизм. Программа при каждом соединении автоматически определяет тип NAT, соответствующий вашей сетевой конфигурации. Вы можете определить тип NAT единовременно, если знаете, что инфраструктура сети не будет изменяться в ближайшее время, тем самым сэкономив несколько секунд при каждом запуске, которые программа тратит на определение.

В редких случаях тип NAT может определяться неправильно, и вы можете указать его вручную. Но помните, что указание неправильного типа NAT может привести к увеличению времени установки прямого соединения с другим абонентом, неоправданной маршрутизации трафика через транзитный сервер, и увеличению задержки речи и количества пропавших пакетов.

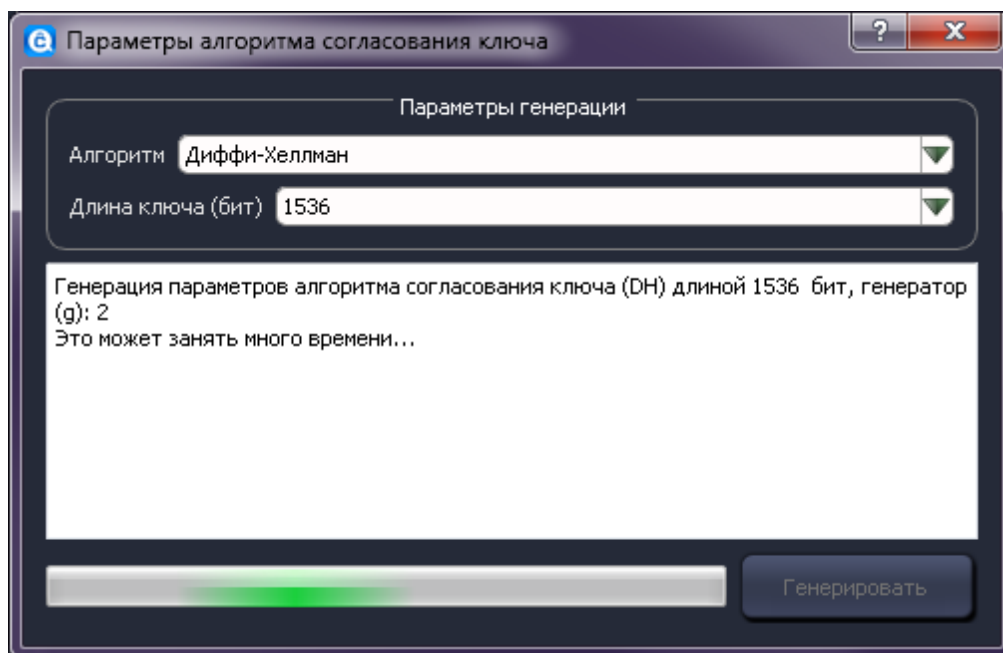
8.5 Вкладка Шифрование



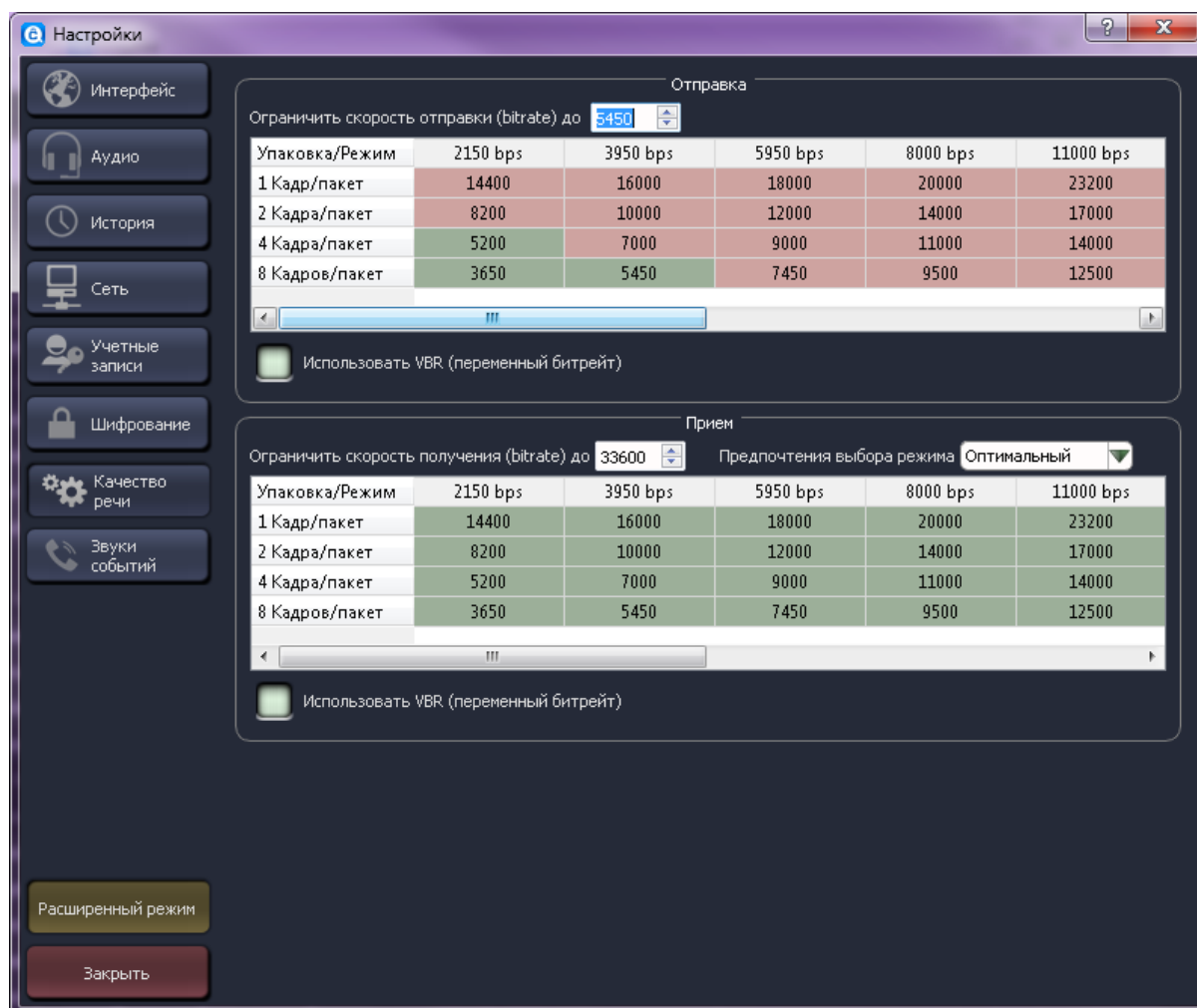
Алгоритмы согласования ключей используются при установке исходящего соединения. Таких алгоритмов может быть несколько, и они будут использоваться в порядке приоритетности. Стрелки справа от списка позволяют устанавливать этот приоритет — верхние программа предпочитает использовать в первую очередь.

Также возможно [вручную](#) занести в кеш набор параметров подключения другого пользователя, минуя процесс согласования по сети.

Если вы озабочены максимальной эффективностью, желательно иметь хотя бы по одному набору параметров по алгоритму «Диффи-Хеллман» и «Диффи-Хеллманн на эллиптических кривых». Вы можете создать новый набор параметров, а также импортировать и экспортировать уже созданный набор с помощью соответствующих кнопок сверху окна. Также как и с парами ключей, процесс генерации набора параметров может занять от нескольких секунд до нескольких десятков минут в зависимости от указанного алгоритма.



8.6 Вкладка Качество речи — контроль потребляемого трафика



Здесь вы можете установить максимальный битрейт голосового канала, что напрямую влияет на качество речи и на потребляемый трафик. Чем выше битрейт — тем лучше качество речи и тем больше трафика расходуется при разговоре.

Звуковые данные оцифровываются с частотой 8 kHz и сжимаются алгоритмом сжатия речи Speex с длиной кадра 20 мсек, который поддерживает несколько режимов сжатия речи. Использование переменного битрейта позволяет существенно снизить потребляемый трафик при сохранении качества речи благодаря тому, что происходит переход на низший битрейт в моменты пауз между словами и некоторых других случаях. Трафик сокращается примерно на 30% в случае кодирования звукового потока с непрерывной речью, и почти в два раза при обычном разговоре (в режиме "один говорит — другой слушает, потом наоборот"). Выбрав переменный битрейт, можно задать самый большой битрейт, который алгоритм может использовать, и тогда звуковые кадры будут кодироваться в этом или меньшем битрейте.

Существуют разные мнения по поводу криптостойкости голосового канала при использовании переменного битрейта, но по нашему мнению, снижение безопасности кодирования в этом случае несущественно. Рекомендуем ознакомиться со [статьей](#) в блоге проекта Cryptia. Помимо прочего, в ней представлены дополнительные технические данные для тех, кто хочет совершить тонкую

настройку.

Каждый из пользователей, участвующих в разговоре, может в своем клиенте ограничить максимальную скорость передачи и приема данных (по умолчанию ограничение установлено на 36800 бит/сек, что фактически означает отсутствие любых ограничений). На этапе установления соединения клиенты Cryptia «договариваются» между собой о том, кто с какой скоростью будет передавать речевые данные, а также выбирает режим получения звуковых данных. Ваши предпочтения по этому режиму вы можете установить в настройках качества речи, используя соответствующий выпадающий список в правом верхнем углу поля Прием. Этот параметр абсолютно субъективен: одним пользователям комфортнее общаться, когда задержка минимальная, другим комфортнее общаться с наилучшим качеством речи, не обращая внимания на задержку. «Оптимальный» режим является разумным (по мнению авторов) компромиссом между этими двумя крайностями..

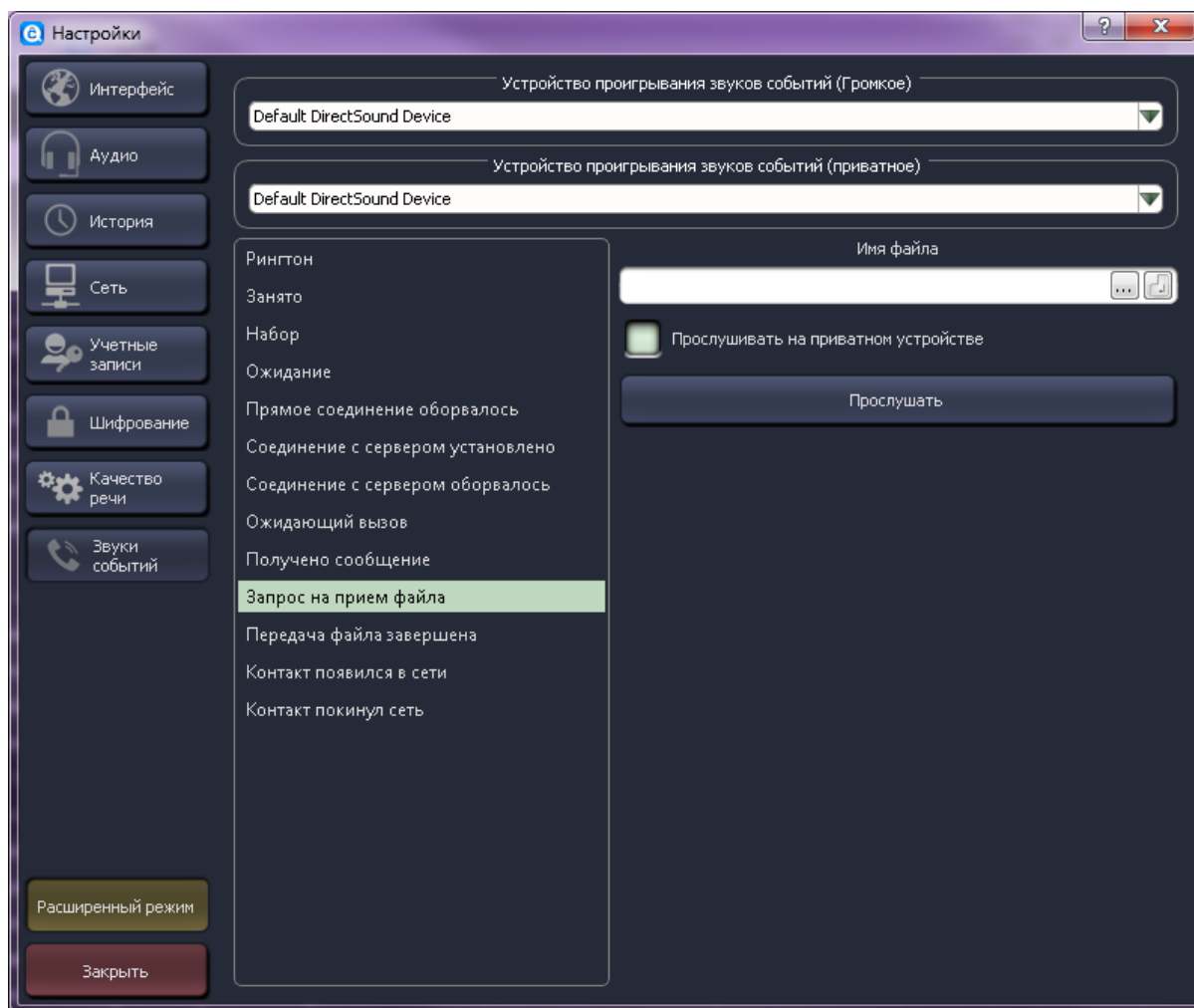
Например если в клиенте А установлено ограничение на передачу на 20000 бит/сек, а в Клиенте В установлено ограничение на прием на 17000 бит/сек, то передача в направлении от Клиента А к клиенту В будет осуществляться со скоростью не более 17000 бит/сек. В таблице ниже используемые режимы отмечены зеленым цветом.

	Режим 0 2150 бит/сек	Режим 1 3950 бит/сек	Режим 2 5950 бит/сек	Режим 3 8000 бит/сек	Режим 5 11000 бит/сек	Режим 7 15000 бит/сек	Режим 9 18200 бит/сек	Режим 10 24600 бит/сек
1 Кадр / пакет	14400	16000	18000	20000	23200	27200	30400	36800
2 Кадра / пакет	8200	10000	12000	14000	17000	19600	24200	30600
4 Кадра / пакет	5200	7000	9000	11000	14000	18000	21200	27600
8 Кадров / пакет	3650	5450	7450	9500	12500	16500	19700	26100

В случае если получатель предпочитает получать звуковые данные с минимальной задержкой, то будет выбран режим 1 (3950 бит/сек) и упаковка по 1 кадру на пакет. Если получатель предпочитает получать звук наилучшего качества, с большей задержкой, то будет выбран режим 7 (15000 бит/сек) и упаковка по 8 кадров / пакет. В оптимальном режиме будет выбран режим 5 (11000 бит/сек) и упаковка по 2 кадра в пакете. Режим 0 (2150 бит/сек) не используется из-за того что качество речи при этом неудовлетворительное, однако алгоритм Speex может переходить в этот режим в случае использования переменного битрейта (в паузах и т.п.).

8.7 Вкладка Звуки событий

В этой вкладке вы можете выбрать звуковую карту, которая будет использоваться для рингтонов, а также сами звуки для различных событий.



В списке слева вы можете выбрать события, к которым необходимо присвоить тот или иной рингтон. Кнопка *Прослушать* справа от списка сыграет установленный для данного события звук. В соответствующем поле выше можно задать файл с желаемым звуком для данного события — выбор происходит в стандартном для операционной системы диалоговом окне, вызываемом кнопкой с тремя точками. Поддерживаются звуковые файлы в форматах .wav и .mp3.

Кнопка сброса  вернет звук события, используемый по умолчанию..

9 Возможности для экспертов

9.1 Редактирование файла Cryptia.ini

Некоторые специфические и крайне редко применимые настройки можно изменить только при помощи редактирования конфигурационного файла *cryptia.ini*. Это сделано для того, чтобы не очень квалифицированные пользователи не могли «донастраивать» программу до полностью неработоспособного состояния. Надеемся, что вы понимаете, что делаете, и, в любом случае, мы не отвечаем за работоспособность программы после редактирования конфигурационного файла. Рекомендуем сохранить резервную копию конфигурационного файла перед началом экспериментов.

Переадресация

Можно вставить в конфигурационный файл cryptia.ini строку с переадресацией в другое место:

```
[redirect]
cryptia.ini=новый_путь/cryptia.ini
```

Это может оказаться полезным в Linux для переадресации файла в папку с другими параметрами доступа.

Изменение пути и имени файла со списком контактов

В разделе [имя_вашего_компьютера] создайте параметр

```
addressBook=<Полный или относительный путь к файлу списка контактов>
```

Если путь к файлу не указан, программа сперва проверяет его наличие в своей папке, и в случае неудачи следует в личную папку пользователя (в операционной системе Windows путь по умолчанию выглядит C:\пользователи\[Имя пользователя]\Appdata\Roaming\Cryptia). Если файл не найден и в этом месте, он будет здесь создан.

Принуждение на работу через заранее запрограммированные UDP порты

Это может потребоваться в случаях, если в вашей сети администратором заведены очень жесткие правила, например, тотально запрещен udr (кроме DNS запросов), но администратор может запрограммировать для вас исключение с указанием udr портов. Или же вы имеете симметричный роутер, и администратор может для вас «пробросить» порты.

```
[serverConnections]
forceToPorts=true
firstPreprogrammedPort=41000
lastPreprogrammedPort=41010
```

По умолчанию это свойство отключено.

Программа при старте займет этот диапазон UDP портов, для того чтобы их случайно не заняла какая-то другая программа. В случае если это свойство установлено в true программа не тестирует NAT, а считает, что вы работаете без NAT.

Таймаут удержания соединения

По умолчанию клиентская программа шлет на сервер специальный пакет keepAlive каждые 45 сек, для того чтобы удерживать соединение с сервером. Если не прислать такой пакет в течении 60 сек неактивности, то сервер разорвет соединение.

```
[serverConnections]
keepAliveTimeout=45000
```

Выбор алгоритмов симметричного шифрования

В раздел encryption конфигурационного файла можно добавить строку со списком поддерживаемых симметричных алгоритмов шифрования в порядке предпочтения. Например:

[encryption]

supportedVoiceCiphers=aes-256;camellia-256;cast-5;seed;des3;bf;

supportedDataCiphers=aes-256;camellia-256;cast-5;seed;

Добавлять можно любые алгоритмы, поддерживаемые библиотекой openssl, идущей в комплекте с программой или установленной в вашей системе.

Если эти строки не заданы, то подразумевается- aes-256 (по умолчанию).

Если в вашей строке не указать aes-256, то вы не сможете общаться с клиентами, которые не производят у себя такую же настройку этих параметров с указанием общих алгоритмов симметричного шифрования.