



Мена'ан
by Inferima.x2 team

РУКОВОДСТВО
ПОЛЬЗОВАТЕЛЯ

2012 ГОД

Все права на Мена'an,
сопутствующие материалы и
ресурсы, включая данное
руководство, принадлежат
Interima.x2 team

GNU GPL v.2/3



"Нужно бежать со всех ног, чтобы
оставаться на месте, а чтобы куда-то
попасть, надо бежать как минимум вдвое
быстрее."

Льюис Кэрролл. Лиса в Зазеркалье.

"Пожалуйста почувствуй нашу боль..."

Interima.x2.



Оглавление

О программе	5
Что такое Mena'an?	5
Разработчики	5
Лицензия	6
Главная	7
Общий обзор	7
Криптографические алгоритмы	8
Создание задачи	10
Задачи	13
Общий обзор	13
Контроль задач	16
Настройки	17
Общий обзор	17
Описание опций	18
Помощь	20
Выход	21
От разработчиков	22



О программе

Что такое Mena'an

Mena'an - это криптографический инструмент для безопасности хранения и передачи ваших данных. Mena'an использует графическую библиотеку Qt 4.8. Mena'an был создан специально для операционной системы Linux, но вы можете использовать его на любой платформе поддерживаемой Qt.

Разработчики

Mena'an был создан командой Interima.x2:

Interima.ix2
Interima.Cry
Interima.Inmay
Interima.Cemetery
Interima.Tombstone
Interima.BlueIceScream
Interima.The Heavy Rain

E-Mail: Interima.x2@gmail.com



Лицензия

This program is Free Software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.



Главная

Общий обзор

Вкладка 'Главная' - это первая вкладка, которую вы видите при запуске приложения. Она показана на рис.1. Это основная вкладка Mena'an, с которой вы начинаете свою работу. Она содержит список доступных криптографических алгоритмов. Для просмотра всего списка, вы можете использовать колесико мыши, либо двигая мышь в вертикальном направлении, удерживая левую кнопку. Справа находится полоса прокрутки, которая показывает в какой части списка вы находитесь. Не пытайтесь использовать ее для прокрутки списка. Она просто выполняет информационную роль.

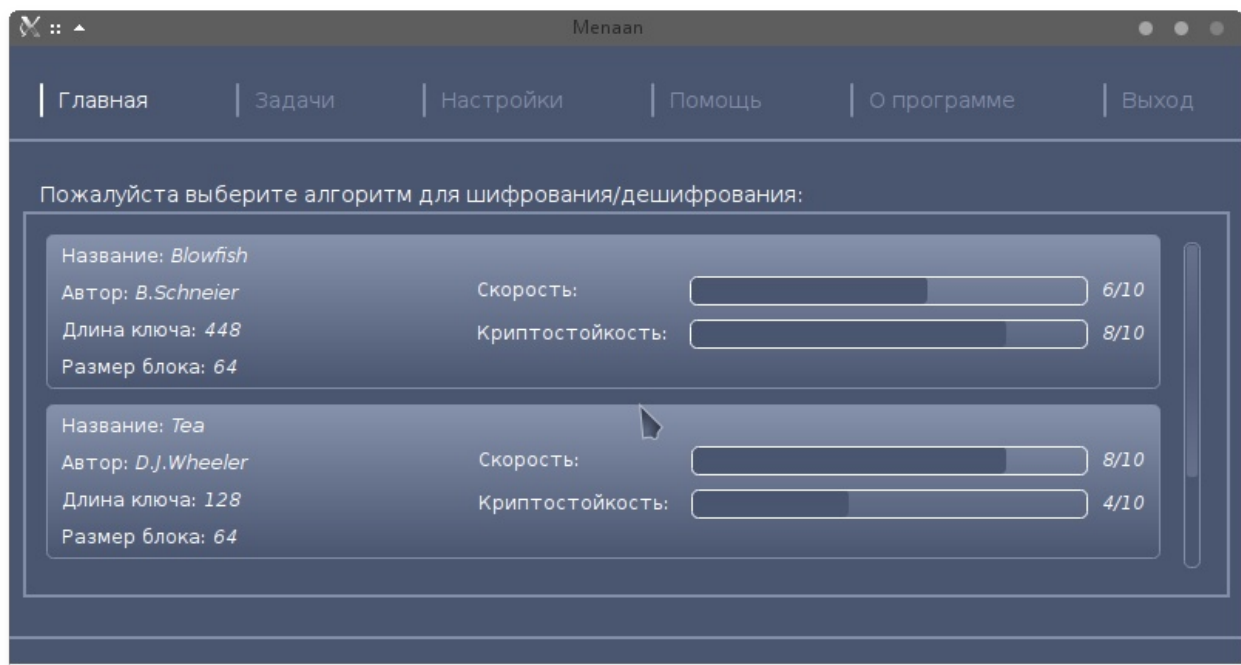


Рис.1. Вкладка 'Главная'



Криптографические алгоритмы

Криптографические алгоритмы реализованы как расширения для основного приложения. Таким образом, они независимы от самого приложения. Вы можете написать свое расширение или получить дополнительное для Mena'an. Так как расширения независимы от приложения, то вы можете скачать и скопировать их в папку 'plugins' директории установки Mena'an. После перезагрузки приложения, новые расширения появятся в списке криптографических алгоритмов. Для различных операционных систем, названия файлов расширений может быть разным. Вы можете получить дополнительные расширения с сайта разработчиков.

Каждый алгоритм характеризуется различными свойствами. Эти свойства отображаются на элементе списка, для каждого алгоритма. Они позволяют вам выбрать алгоритм, который вас устраивает. На рис.2. показан один из элементов списка, соответствующий алгоритму 'Tea'.

'Название' - это поле содержит международное название криптографического алгоритма.

'Автор' - это поле содержит автора алгоритма. Если авторов алгоритма много, то указывается только один из них. Не путайте автора криптографического алгоритма, с автором расширения, которое реализует этот алгоритм.

Название: <i>Blowfish</i>	Скорость:	<div><div></div></div>	6/10
Автор: <i>B.Schneier</i>	Криптостойкость:	<div><div></div></div>	8/10
Длина ключа: 448			
Размер блока: 64			

Рис.2. Информация об алгоритме

'Длина ключа' - это поле содержит размер ключа криптографических преобразований в битах. Большой размер ключа, обладает большим запасом криптостойкости к некоторым видам атак.

'Длина блока' - это поле указывает размер блока данных для блочных алгоритмов. Размер блока данных указывается в битах и показывает какими порциями данных оперирует алгоритм. Большой размер блока данных имеет некоторые преимущества в криптостойкости алгоритма.

'Скорость' - это поле отображает скоростные характеристики алгоритма. Это очень важная характеристика. Некоторые алгоритмы, производят свои операции с данными очень долго, другие, наоборот быстро. Обычно скорость алгоритма зависит от его сложности. Чем сложнее алгоритм, тем дольше он работает. Однако для большинства алгоритмов действует правило: чем быстрее скорость работы, тем слабее криптостойкость. Данная характеристика не является стандартной. Она просто используется разработчиками для облегчения выбора пользователем необходимого ему алгоритма. Минимальное значение скорости равно 1, а максимальное равно 9.

'Криптостойкость' - это поле отображает криптографическую стойкость алгоритма, то есть его возможности противостоять взлому. Оценка криптостойкости выдается на основе криптоанализа алгоритма. Это еще одна очень важная характеристика. Если вы нуждаетесь в экстремальном уровне защиты ваших данных, то выбирайте алгоритмы с максимальной криптостойкостью. Однако не забывайте правило для большинства алгоритмов: чем больше степень защиты, тем меньше скорость. Данная характеристика не является стандартной. Она просто используется разработчиками для облегчения выбора пользователем необходимого ему алгоритма. Минимальное значение криптостойкости равно 1, а максимальное равно 9.

Когда вы решили какой алгоритм выбрать, то кликните по нему левой кнопкой мыши в списке.



Создание задачи

После того как вы выберете алгоритм, Мена'ап попросит ввести параметры для создания задачи. Что такое задача? Задача - это запрос для Мена'ап выполнить преобразования с данными, который состоит из алгоритма, входных и выходных данных. Таким образом, выполнение задачи - это преобразование входных данных в выходные по правилам криптографического алгоритма. Форма ввода данных для создания задачи показана на рис.3.

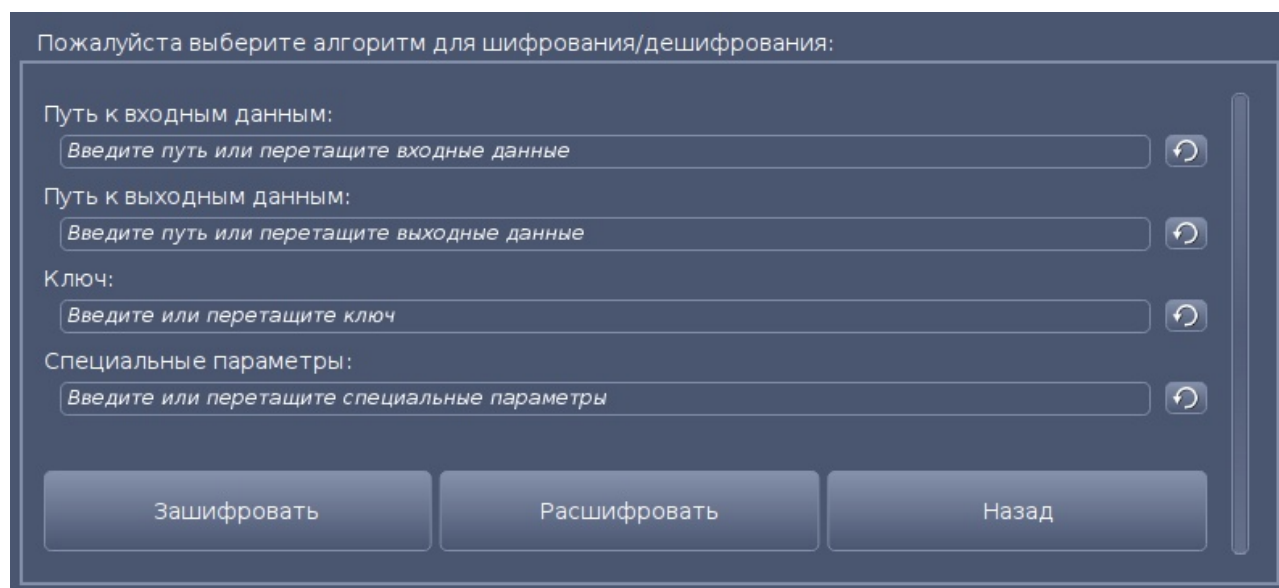


Рис.3. Форма создания задачи

Форма состоит из полей для ввода данных, подписей к ним и кнопок очистки содержимого полей ввода. Также внизу расположены кнопки создания задачи и возврата в предыдущее меню. Рассмотрим каждый элемент формы.

'Путь к входным данным' - в поле под этой подписью, необходимо ввести путь к входным данным. Входными данными могут быть директория или файл. Путь необходимо ввести с клавиатуры или просто перетащить источник входных данных мышкой в это поле.

'Путь к выходным данным' - в поле под этой подписью, необходимо ввести путь к выходным данным, то есть к данным, которые получатся в результате преобразования входных данных. Выходными данными могут быть директория или файл. Если входными данными является директория, то выходными данными, также должна быть директория. Вы можете ввести путь с клавиатуры или перетащить выходные данные. Входные и выходные данные не могут иметь один и тот же путь, если только вы не включили опцию 'Использовать специальное расширение', в настройках программы.

'Ключ' - в это поле необходимо ввести ключ. Что такое ключ? Ключ - это некоторая последовательность символов конечной длины. Ключ позволяет шифровать и расшифровывать данные. Выбирайте сложные ключи и никому не сообщайте их, кроме тех лиц, которые имеют разрешение на расшифровывание или шифрование данных. В качестве ключа, вы можете использовать любые символы, так как Mena'an поддерживает Unicode. Каждый алгоритм имеет определенный размер ключа, с которым он работает. Этот параметр отображен в информации о алгоритме. Если введенный вами ключ слишком мал, то Mena'an циклически будет использовать ваш ключ добиваясь приемлемого размера. Если ключ слишком большой, то Mena'an усечет его длину до приемлемой. Вы можете не волноваться об этом, Mena'an сделает все автоматически и незаметно для вас. Помните, что если вы забудете ключ, вы никогда не сможете расшифровать свои данные.

'Специальные параметры' - это поле является необязательным для заполнения. В это поле можно вводить параметры влияющие на внутреннюю работу алгоритма. Это специфичные параметры для каждого алгоритма, для некоторых алгоритмов они могут отсутствовать. Например, эти параметры могут задавать начальные значения некоторым константам, используемым в алгоритме, задавать режимы работы, количество раундов и так далее. Так как нет стандарта для этих параметров, то каждое расширение для Mena'an должно содержать файл, с описанием возможных специальных параметров. Эти файлы описания имеют название такое же, как и у плагина, с расширением '.txt' и находятся в директории 'description' в директории установки приложения. Если вы не нуждаетесь в специальных параметрах - не заполняйте это поле.



Если вы задали неправильные параметры - не волнуйтесь. Мена'ап проверяет все введенные данные и сообщит вам если вы ошиблись.

После того как все необходимые данные введены, вы можете создать задачу.

'Зашифровать' - эта кнопка, создает задачу в режиме шифрования. При шифровании, Мена'ап вставляет в начало выходного файла специальную последовательность чисел - магическое число. Это необходимо при дешифровании, для идентификации файла.

'Дешифровать' - эта кнопка, создает задачу в режиме дешифрования. Мена'ап считывает магическое число и начинает выполнять задачу. Если считать магическое число не удастся, Мена'ап сообщит об ошибке.

После создания задачи, вы можете продолжать создавать новые задачи с выбранным алгоритмом или вернуться в предыдущее меню списка алгоритмов, нажатием на кнопку 'Назад'.



Задачи

Общий обзор

Все задачи, которые вы создали, отображаются на вкладке 'Задачи'. Эта вкладка изображена на рис.4. Задачи расположены в вертикальном порядке по времени создания. Задачи имеют общий заголовок списка, который описывает столбцы, из которых состоит каждая задача. Заголовок показан на рис.5.

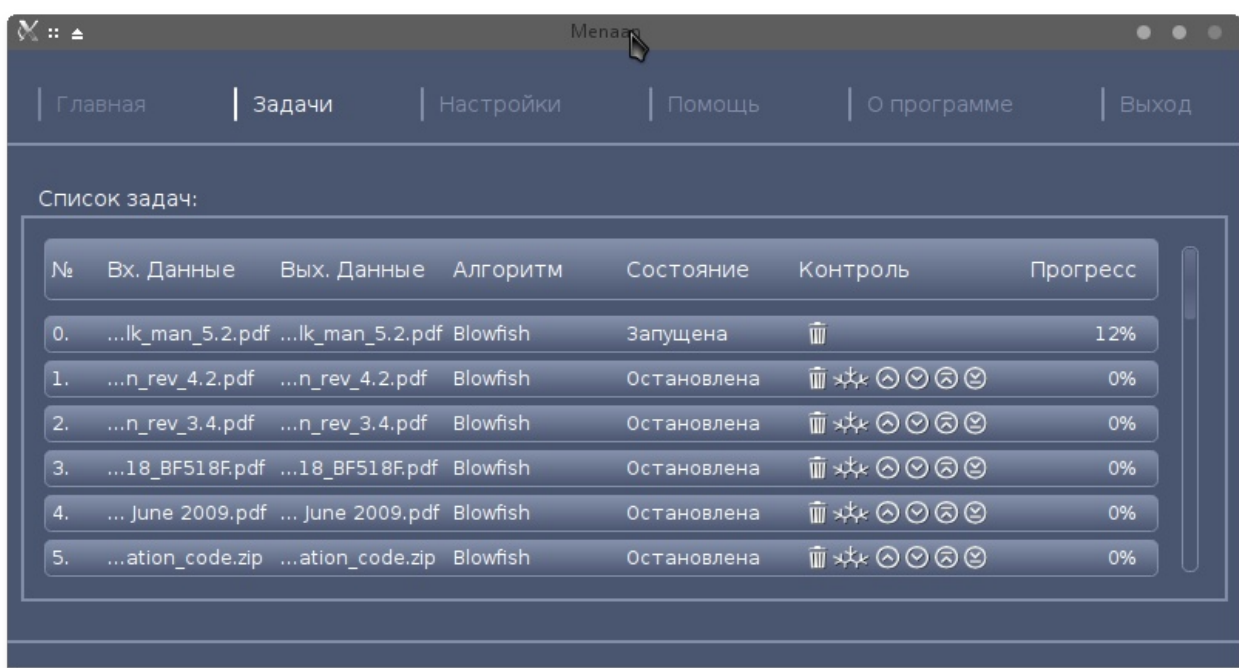


Рис.4. Вкладка 'Задачи'



Рассмотрим все столбцы заголовка задач.

'№' - этот столбец содержит номера созданных задач. Каждая задача имеет уникальный номер. Это значение не является номером задачи в списке. Оно характеризует время создания задачи. Чем больше номер, тем позже была создана задача. Номера задач в списке обычно идут по порядку возрастания, однако, при изменении приоритета задачи, этот порядок может нарушиться.

'Вх. Данные' - этот столбец содержит название источника входных данных, который был указан при создании задачи. Если имя источника входных данных слишком длинное, оно урезается так, чтобы была видна его конечная часть.

'Вых. Данные' - этот столбец содержит название источника выходных данных, который был указан при создании задачи. Если имя источника выходных данных слишком длинное, оно урезается так, чтобы была видна его конечная часть.

№	Вх. Данные	Вых. Данные	Алгоритм	Состояние	Контроль	Прогресс
---	------------	-------------	----------	-----------	----------	----------

Рис.5. Заголовок списка

'Алгоритм' - этот столбец содержит алгоритмы созданных задач.

'Состояние' - этот столбец определяет текущее состояние задачи.

Задача имеет состояния:

'Запущена' - задача выполняется на одном из процессоров в данный момент.



'Остановлена' - задача ожидает возможности запуска на выполнение. Задача запустится, как только появится возможность захватить свободный процессор. Некоторые задачи могут мешать запуску других. Это происходит, например, если задача пользователя ожидает источник входных данных, который является выходными данными для другой запущенной задачи. В таком случае задача будет ожидать завершения всех конфликтующих задач, а затем запустится на выполнение.

'Завершена' - задача успешно завершилась. Такую задачу можно удалять из списка. Все файлы уже сохранены на запоминающем устройстве.

'Заблокирована' - задача была заблокирована пользователем. Такая задача не выполняется, пока пользователь не произведет разблокировку.

'Ошибка' - при выполнении задачи произошла ошибка. Причины ошибки могут быть различными. Например, ошибка при чтении или записи данных, неправильные специальные параметры для алгоритма, крах инициализации плагина, отсутствие магического числа. Menap, при возникновении ошибки, удалит все временные файлы и сообщит об ошибке. Пользователю, следует удалить такую задачу из списка задач, устранить проблему и создать задачу заново.

'Контроль' - этот столбец содержит средства управления задачами. Мы поговорим подробнее о нем в следующей главе.

'Прогресс' - этот столбец показывает прогресс выполнения задачи в процентах. Это значение, для больших входных данных, может меняться очень медленно, и может казаться, что программа зависла, но это не так. В целях оптимизации значение меняется не по 1%, а сразу небольшими порциями. Когда прогресс доходит до значения 100%, то задача считается завершенной.



Контроль задач

Каждая задача имеет столбец с кнопками управления. Задача из списка показана на рис.6.

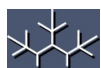


Рис.6. Вид задачи

Рассмотрим значение каждой кнопки управления.



Удаляет задачу из списка задач. Все временные файлы, созданные задачей, будут удалены.



Блокирует задачу. Блокировать можно только не запущенную на выполнение задачу.



Разблокирует задачу. Разблокировать можно только заблокированную задачу.



Присваивает минимальный приоритет задаче. Устанавливает задачу последней в списке задач.



Присваивает максимальный приоритет задаче. Устанавливает задачу первой в списке задач.



Уменьшает приоритет задачи. Проталкивает задачу вниз, в списке задач.



Увеличивает приоритет задачи. Выталкивает задачу вверх, в списке задач.

Настройки

Общий обзор

Настройки приложения содержатся на вкладке 'Настройки'. Эта вкладка показана на рис.7. Вкладка состоит из списка опций. Каждая опция отвечает за определенную функцию в приложении. Опции имеют определенные изменяемые значения. Пользователь может изменять значение каждой опции, используя кнопку с изображением стрелки, около значения опции. Значения опций находятся в циклическом списке. Поэтому, чтобы получить предыдущее значение, пользователю необходимо нажимать кнопку со стрелкой.

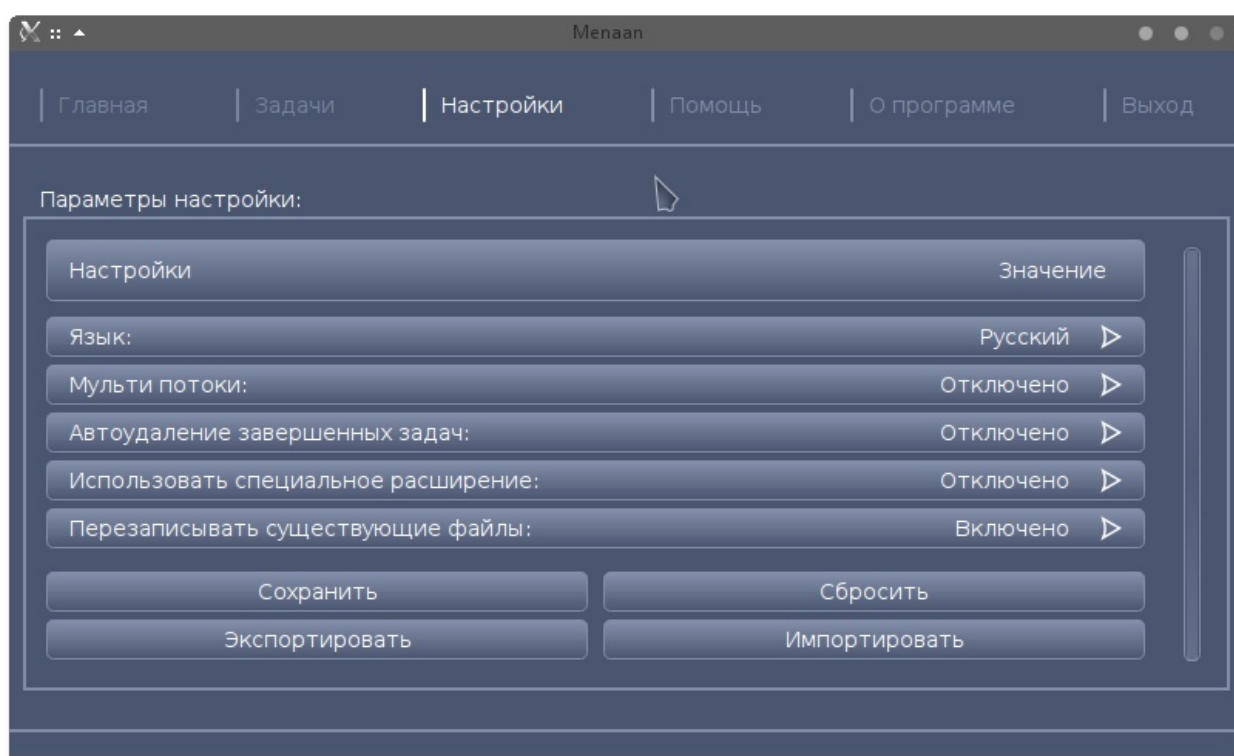


Рис.7. Вкладка 'Настройки'

Описание опций

Опишем каждую опцию по отдельности.

'Язык' - эта опция устанавливает язык приложения. Mena'an позволяет поддерживать несколько языков. Если вы хотите добавить свой перевод приложения обратитесь к разработчикам. По умолчанию, значение этой опции - 'English'.

'Мульти потоки' - эта опция включает или выключает использование программой множества потоков. Каждый поток выполняет отдельную задачу. Чем больше потоков, тем быстрее выполнятся все задачи. Количество потоков определяется по количеству процессорных ядер (в том числе и логических). Если ваш процессор имеет только одно ядро, то будет использоваться только один поток, то есть в каждый момент времени будет выполняться только одна задача. По умолчанию значение этой опции - 'Включено'. Мы рекомендуем использовать именно это значение.

'Автоудаление завершенных задач' - эта опция включает и выключает функцию автоматического удаления задач которые были завершены. То есть, после успешного завершения задачи, она будет удалена из списка, если значение этой опции - 'Включено'. В другом случае, вам придется удалять задачу вручную, в списке задач, воспользовавшись кнопками управления задач. По умолчанию значение этой опции - 'Отключено'.

'Использовать специальное расширение' - это опция включает или выключает функцию дополнения названий выходных данных (файла или директории) специальной записью. Включение этой опции позволяет указывать одинаковые входные и выходные данные для задачи. Mena'an при этой добавит к названию (файла или директории) выходных данных запись с типом выполняемого преобразования. Например для выходного файла шифрующегося с помощью метода ECB, к названию файла добавится строка 'ecb_enc'. По умолчанию значение этой опции - 'Отключено'.



'Перезаписывать существующие файлы' - эта опция включает или отключает функцию перезаписи новыми выходными данными, старых, уже существующих. То есть, если на запоминающем устройстве уже есть файл, с таким же именем, каким указано в качестве выходных данных для задачи, то при включенной опции, старый файл будет перезаписан, все данные которые он хранил пропадут. Более того, данный файл уже будет невозможно восстановить средствами восстановления данных. Будьте внимательны. Если же опция отключена, то при совпадении названий файлов, Mena'an добавит уникальную строку символов в название выходных данных, тем самым сохранит старые данные на запоминающем устройстве. По умолчанию эта опция имеет значение - 'Отключено'.

Будьте внимательны при изменении параметров. Если вы не знаете что делаете - не делайте ничего.

После того, как значения опций были изменены, вы обязательно должны сохранить изменения. Дело в том, что изменения вступят в силу, только после перезапуска приложения.

Кнопка 'Сохранить' позволяет сохранить все изменения. Если изменения успешно сохранены, Mena'an выдаст соответствующее сообщение.

Кнопка 'Сбросить' позволит вернуть настройки по умолчанию. Используйте эту функцию, если вы случайно изменили настройки и хотите вернуть все как было.

Кнопки 'Импорт' и 'Экспорт' позволяют импортировать и экспортировать настройки приложения, соответственно.



Помощь

Вкладка 'Помощь' содержит небольшую справочную информацию по программе. Эта вкладка изображена на рис.8.

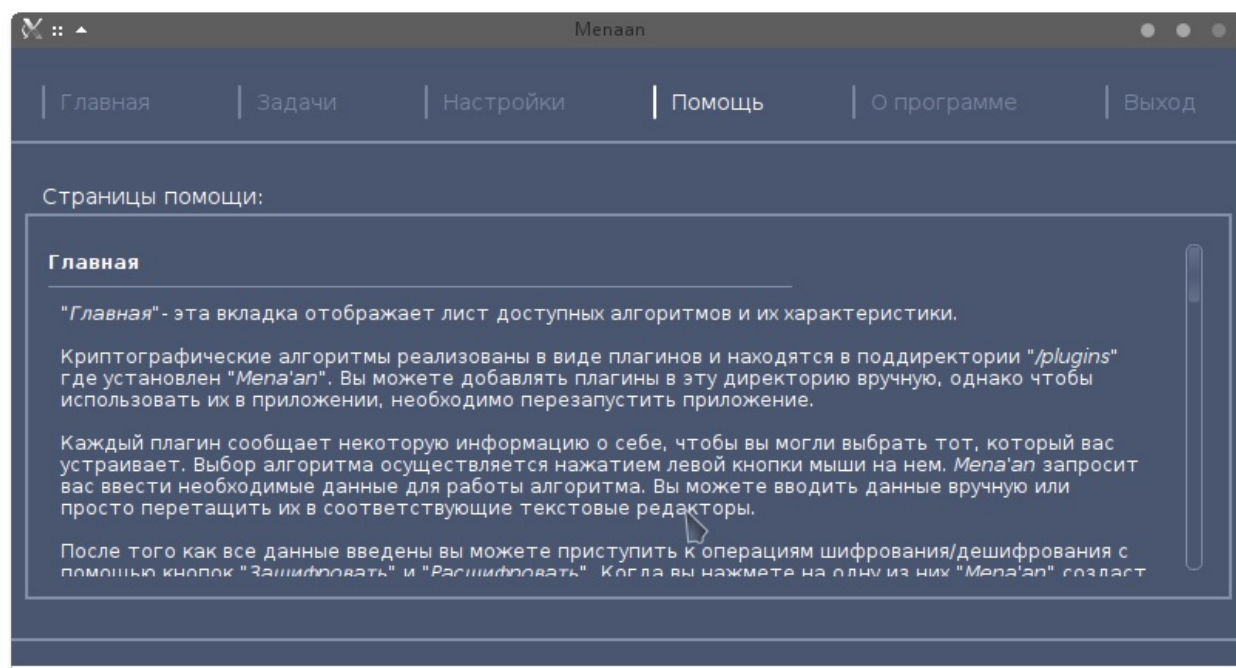


Рис.8. Вкладка 'Помощь'

ВЫХОД

Вкладка 'Выход', предназначена для правильного выхода из программы. В момент выхода из программы могут быть еще не запущенные или выполняющиеся задачи. Если пользователь все же решил выйти, то все задачи будут остановлены и удалены принудительно. Все временные данные также будут удалены. Будьте осторожны, иначе потеряете свои данные. Эта вкладка изображена на рис.9.

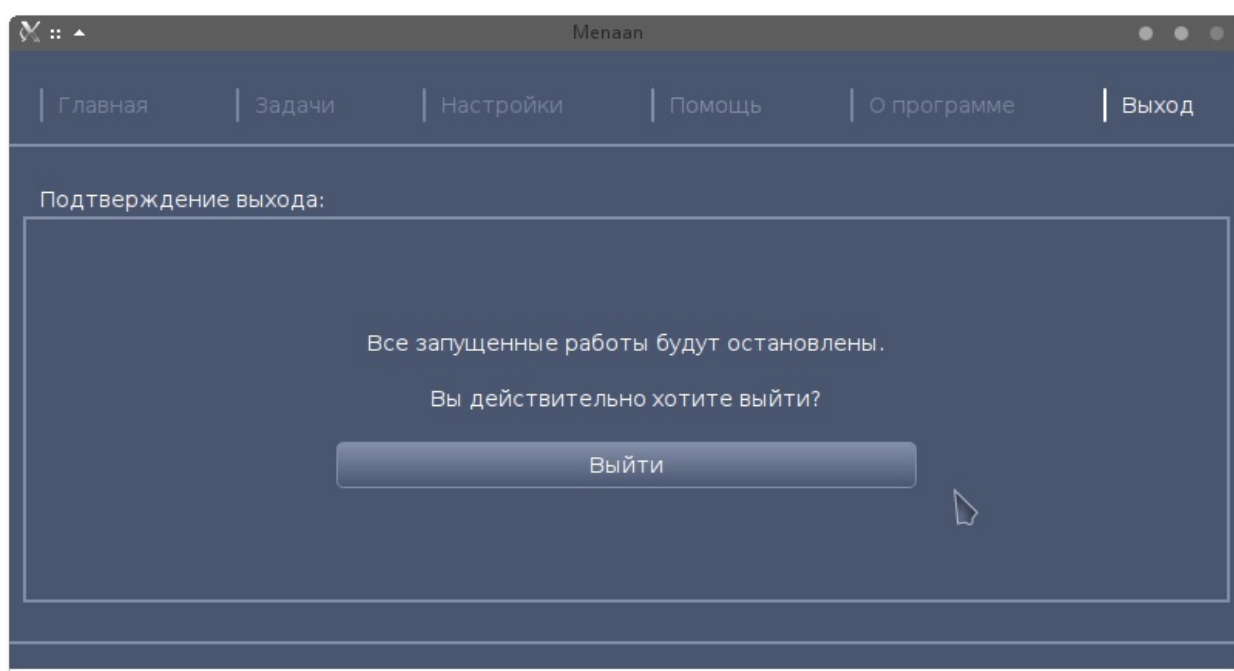


Рис.9. Вкладка 'Выход'



От разработчиков

Mena'an является развивающимся продуктом, поэтому содержит большое количество ошибок, неоптимизированного кода и решений.

Обнаруженные ошибки, предложения или конкретный код отправляйте разработчикам. Mena'an требует увеличения количества плагинов-алгоритмов. Некоторые заявленные возможности могут отсутствовать, временно. Если у вас есть возможность, вы можете написать свои плагины, либо способствовать переводу.

Если у вас есть работа для разработчиков напишите нам.

Для разработки плагинов прочтите файл: 'PluginHowTo.pdf' в директории 'develop'. Все возникшие вопросы задавайте разработчикам.

Interima.x2 team - это один человек. Не забывайте. Не всегда возможно сразу отвечать на вопросы. Проявляйте терпение.

E-mail: interima.x2@gmail.com

Блог разработчиков: exsector.blogspot.com/menaan.html

Исходный код: git.interima.x2/menaan/

