**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ**

**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**

**«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Факультет компьютерных наук

Департамент программной инженерии

|  |  |  |
| --- | --- | --- |
| СОГЛАСОВАНО  профессор департамента программной инженерии, канд. техн. наук  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.В. Шилов  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. |  | УТВЕРЖДАЮ  Академический руководитель образовательной программы «Программная инженерия»    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.В. Шилов  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл*** | **RU.17701729.5071102 -01 34 01-1** | | **ПРОГРАММА ДЛЯ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ**  **С ПОМОЩЬЮ РЕШЕТКИ КАРДАНО**  **Руководство оператора**  **ЛИСТ УТВЕРЖДЕНИЯ**  **RU.17701729.5071102-01 34 01-1-ЛУ** | | |
|  |  | |
| Исполнитель:  студент группы БПИ177  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Данилов А.А. /  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. | |
|  | | |
|  | |  |

**2018**

|  |  |  |  |
| --- | --- | --- | --- |
| **УТВЕРЖДЕНО**  **RU.17701729.5071102-01 34 01-1-ЛУ** | |  |  |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл*** | **RU.17701729.5071102-01 34 01-1** | | **ПРОГРАММА ДЛЯ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ**  **С ПОМОЩЬЮ РЕШЕТКИ КАРДАНО**  **Руководство оператора**  **RU.17701729.5071102-01 34 01-1**  **Листов 13** | | | | |
|  |  | | | |
|  | | | |
|  | | | | |

**2018**

|  |  |  |
| --- | --- | --- |
|  |  |  |

СОДЕРЖАНИЕ

[1. Назначение программы..........................................................................................................4](#_Toc514329557)

[**1.1 Функциональное назначение** 4](#_Toc514329558)

[**1.2 Эксплуатационное назначение** 4](#_Toc514329559)

[2. Условия выполнения программы........................................................................................4](#_Toc514329560)

[**2.1 Минимальный состав аппаратных средств** 4](#_Toc514329561)

[**2.2 Минимальный состав программных средств** 4](#_Toc514329562)

[**2.3 Требования к персоналу (пользователю)** 3](#_Toc514329563)

[3. Выполнение программы........................................................................................................3](#_Toc514329564)

[**3.1 Установка программы** 3](#_Toc514329565)

[**3.2 Запуск программы и работа с приложением** 3](#_Toc514329566)

[**3.2.1 Редактор решетки** 5](#_Toc514329567)

[**3.2.2 Шифратор информации:** 6](#_Toc514329568)

[**3.2.3 Дешифратор информации** 6](#_Toc514329569)

[**3.2.4 Чат** 7](#_Toc514329570)

[**3.2.5 Помощь** 8](#_Toc514329571)

[**3.2.6 О программе** 8](#_Toc514329572)

[ПРИЛОЖЕНИЕ 1........................................................................................................................9](#_Toc514329573)

[ПРИЛОЖЕНИЕ 2......................................................................................................................10](#_Toc514329574)

[ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ................................................................................11](#_Toc514329575)

# **1. Назначение программы**

## **1.1 Функциональное назначение**

Программа предоставляет пользователю создавать собственные решетки Кардано. После того как пользователь создаст решетку, он может шифровать и дешифрировать информацию с помощью этой решетки. Также программа предоставляет пользователям возможность создавать собственный сервер чата и обмениваться в нем зашифрованными сообщениями с другими подключенными пользователями.

## **1.2 Эксплуатационное назначение**

Программа демонстрирует процесс и результат шифрования и дешифрования методом решетки Кардано, а также дает возможность пользователю исследовать некоторые их особенности.

Конечными пользователями программы могут быть научные деятели, преподаватели, а также студенты, интересующиеся кодированием, в частности методом решетки Кардано.

# **2. Условия выполнения программы**

## **2.1 Минимальный состав аппаратных средств**

1. Персональный компьютер, оснащенный процессором с тактовой частотой 1 ГГц и выше;
2. 200 Мб свободного места на жёстком диске.
3. Монитор с разрешением 1024x768 или выше.
4. Мышь или другое совместимое указывающее устройство;
5. Клавиатура;

## **2.2 Минимальный состав программных средств**

1. Операционная система Microsoft Windows 7 или более поздняя версия Windows;
2. Должен быть установлен .NET Framework версии не ниже 2.0;

## **2.3 Требования к персоналу (пользователю)**

Особых требований к пользователю не предъявляется.

# **3.** **Выполнение программы**

В данном разделе описан пример работы с программой.

## **3.1 Установка программы**

Для установки программы необходимо скопировать папку «CardanoGrill» с информационного накопителя на компьютер.

## **3.2 Запуск программы и работа с приложением**

Приложение запускается при открытии файла “CardanoGrill.exe”. После запуска появляется окно для выбора языка(рис. 1).

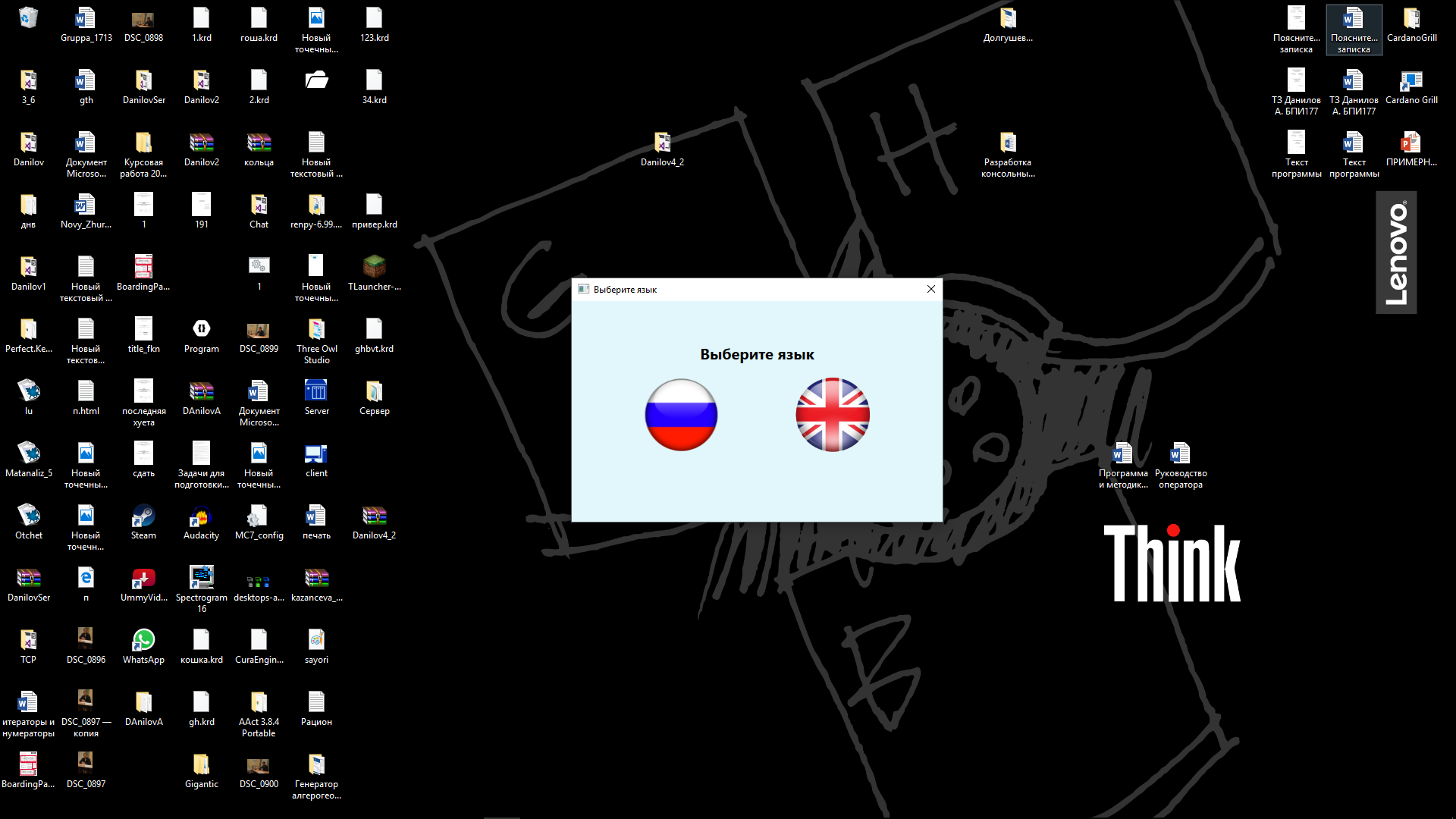
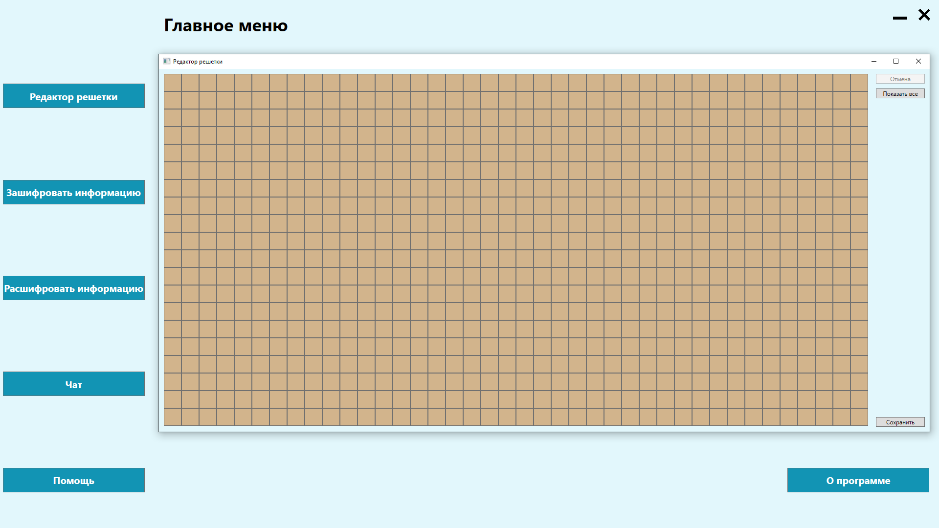


Рисунок 1. MainWindow

Для начала работы нужно выбрать желаемый язык: Английский или Русский.

После выбора языка откроется главное меню (рис. 2)

8

7

6

5

4

3

2

1

Рисунок 2. MainMenu

При нажатии на кнопку 1 откроется редактор решетки, при нажатии на кнопку 2 откроется шифратор информации, при нажатии на кнопку 3 откроется дешифратор решетки, при нажатии на кнопку 4 откроются настройки чата, при нажатии на кнопку 5 откроется помощь, при нажатии на кнопку 6 откроется информация о программе, при нажатии на кнопку 7 свернется окно, при нажатии на кнопку 8 закроется окно.

Кнопки 1-4 изначально открывают настройку каждого из соответствующих окон (рис. 3). В появившемся окне пользователь вводит размер решетки.

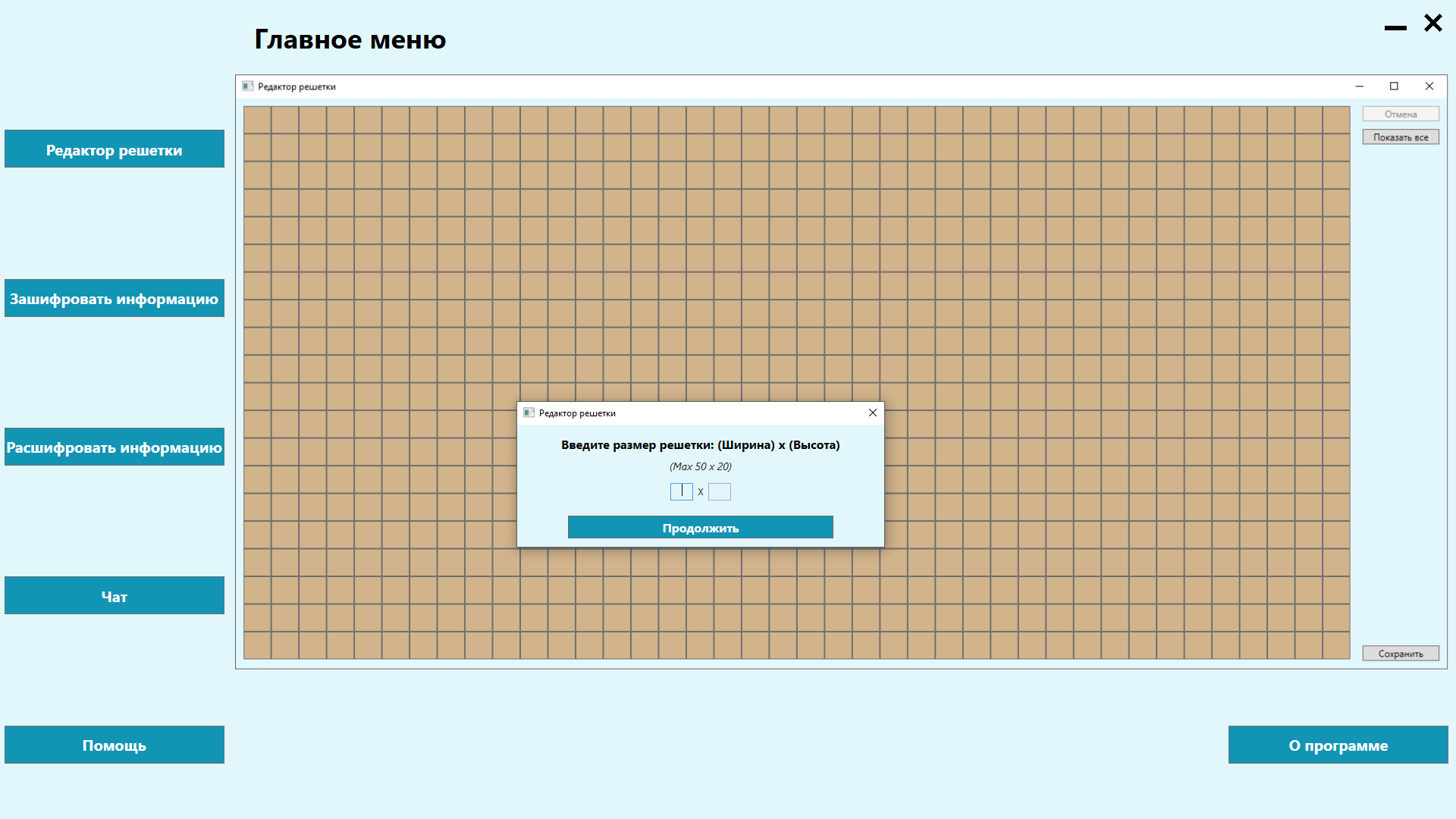
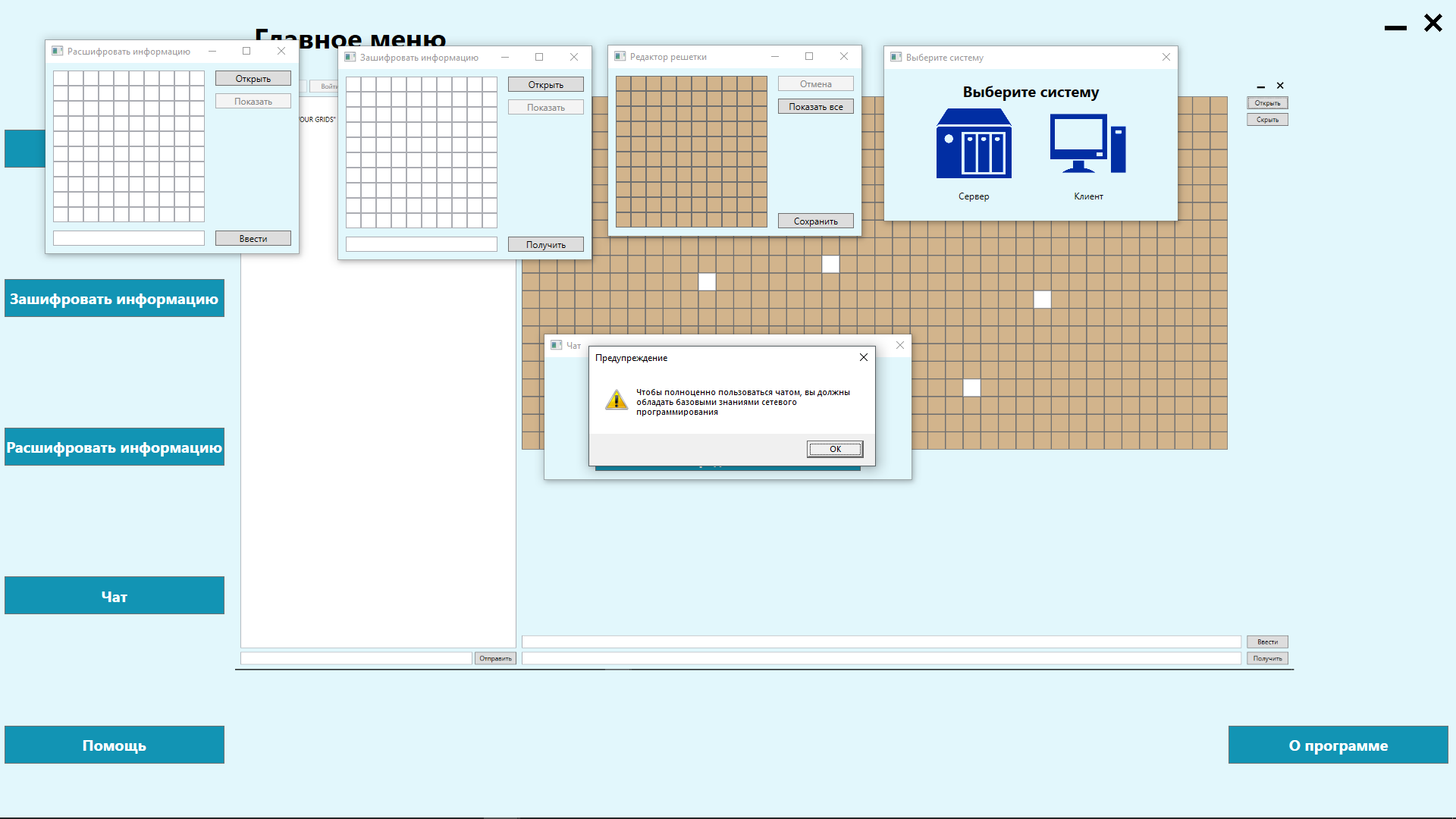
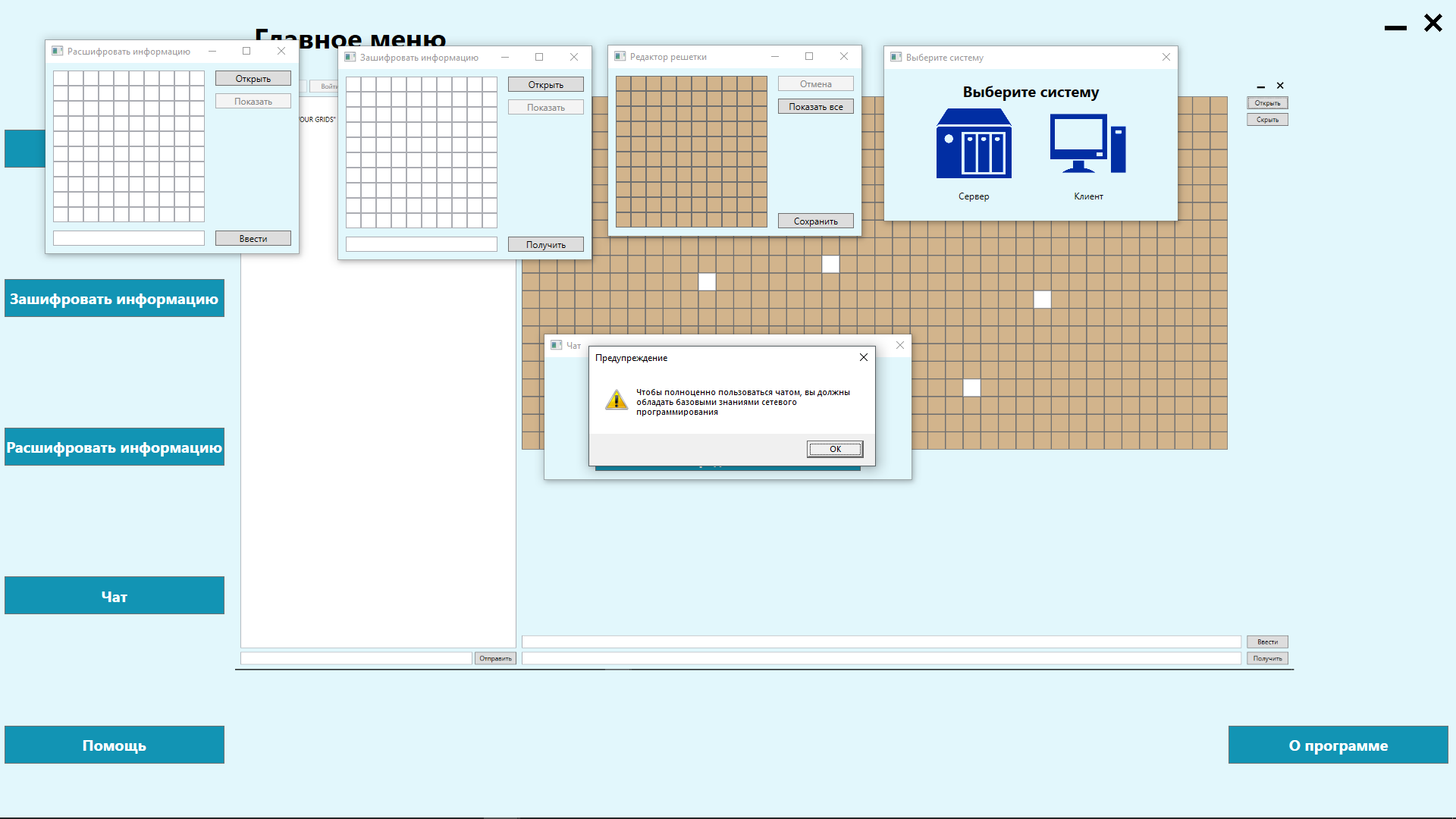
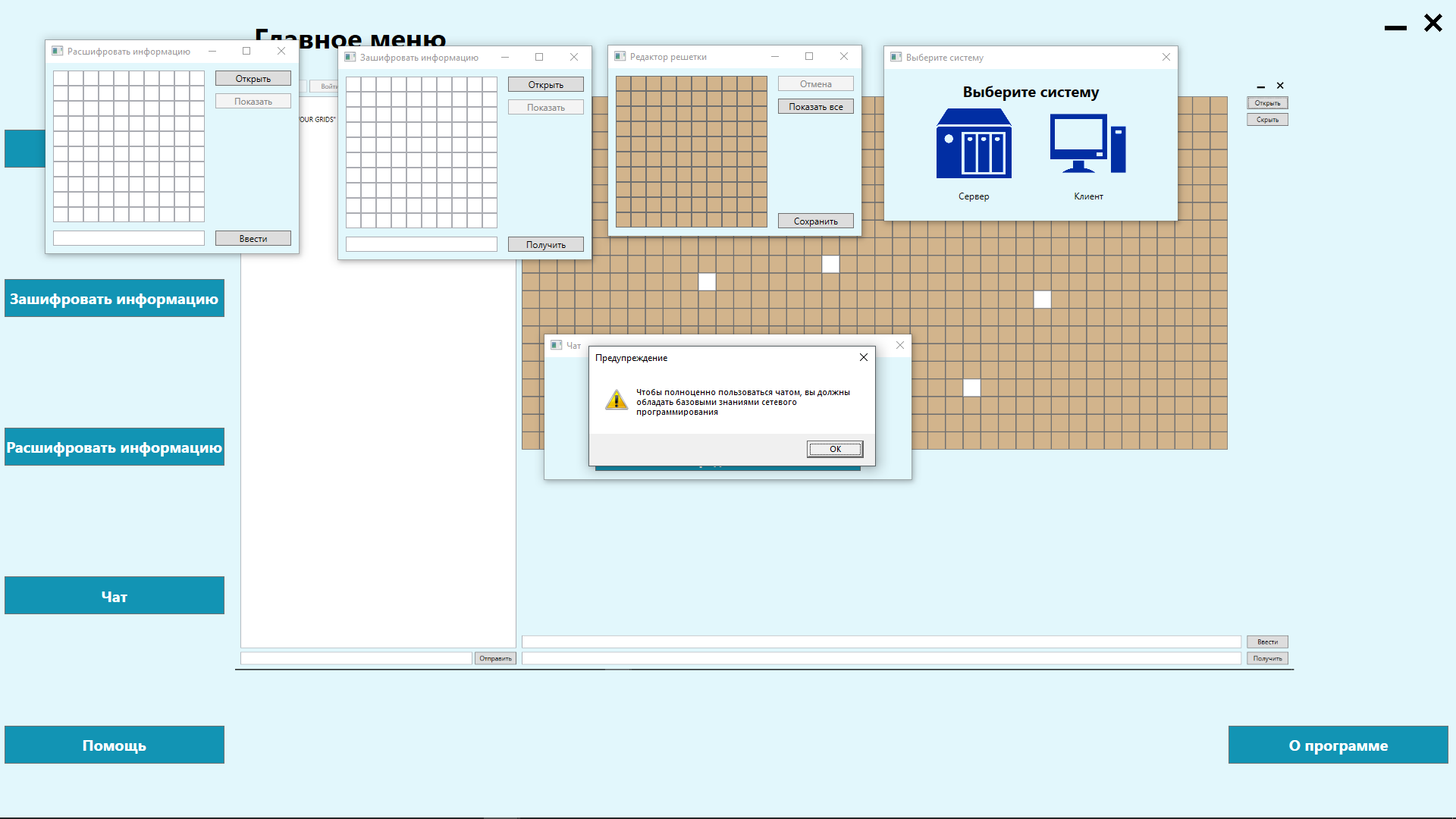


Рисунок 3. EnteringField (выбран редактор решетки)

После ввода размера открывается редактор решетки (рис. 6)/шифратор информации (рис. 5)/дешифратор информации (рис. 4)/настройки чата (рис. 8)

Если пользователь выбрал чат, то появляется предупреждение (рис. 7), что пользователю необходимы базовые знания для полноценного создания чата.



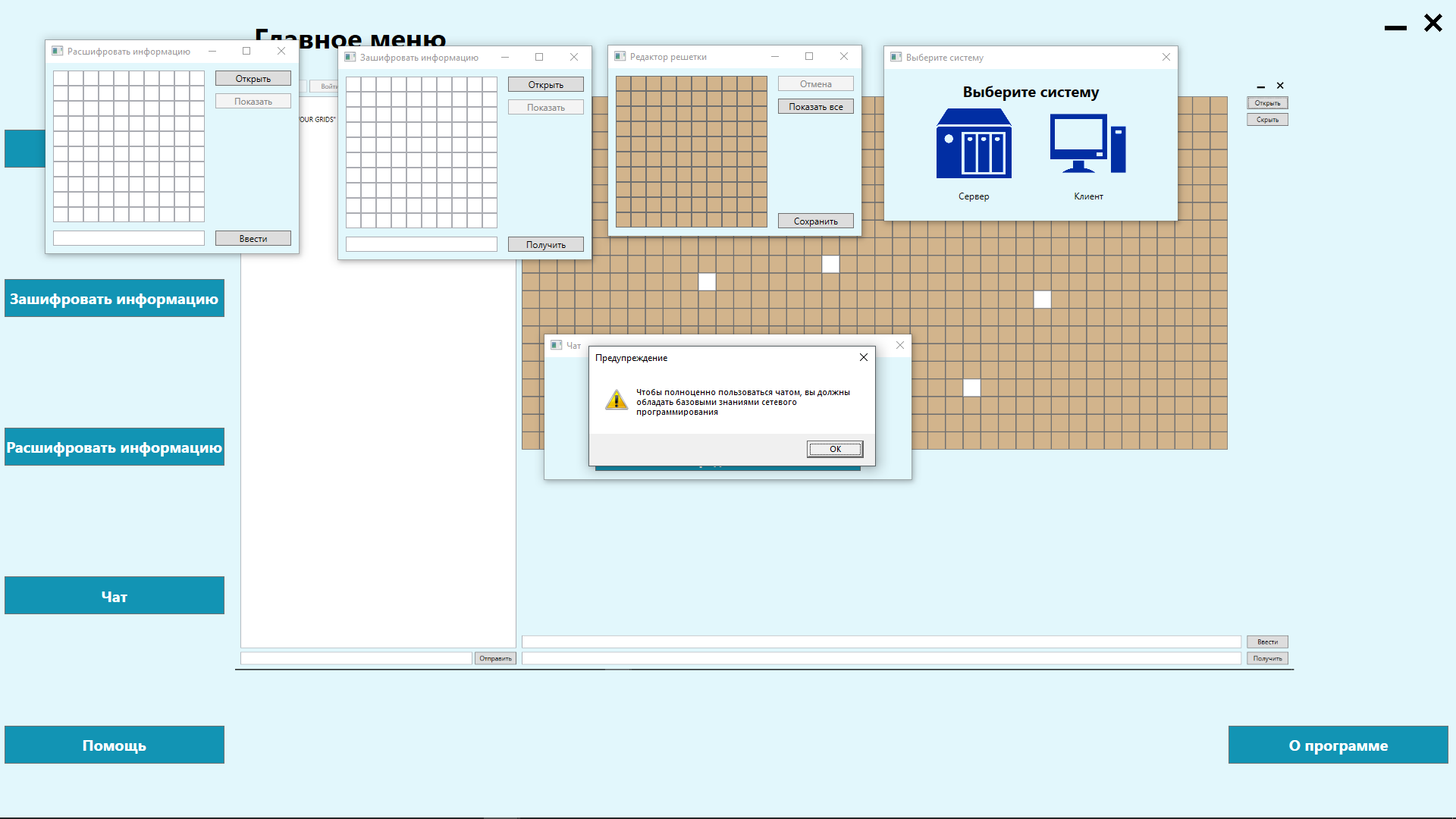
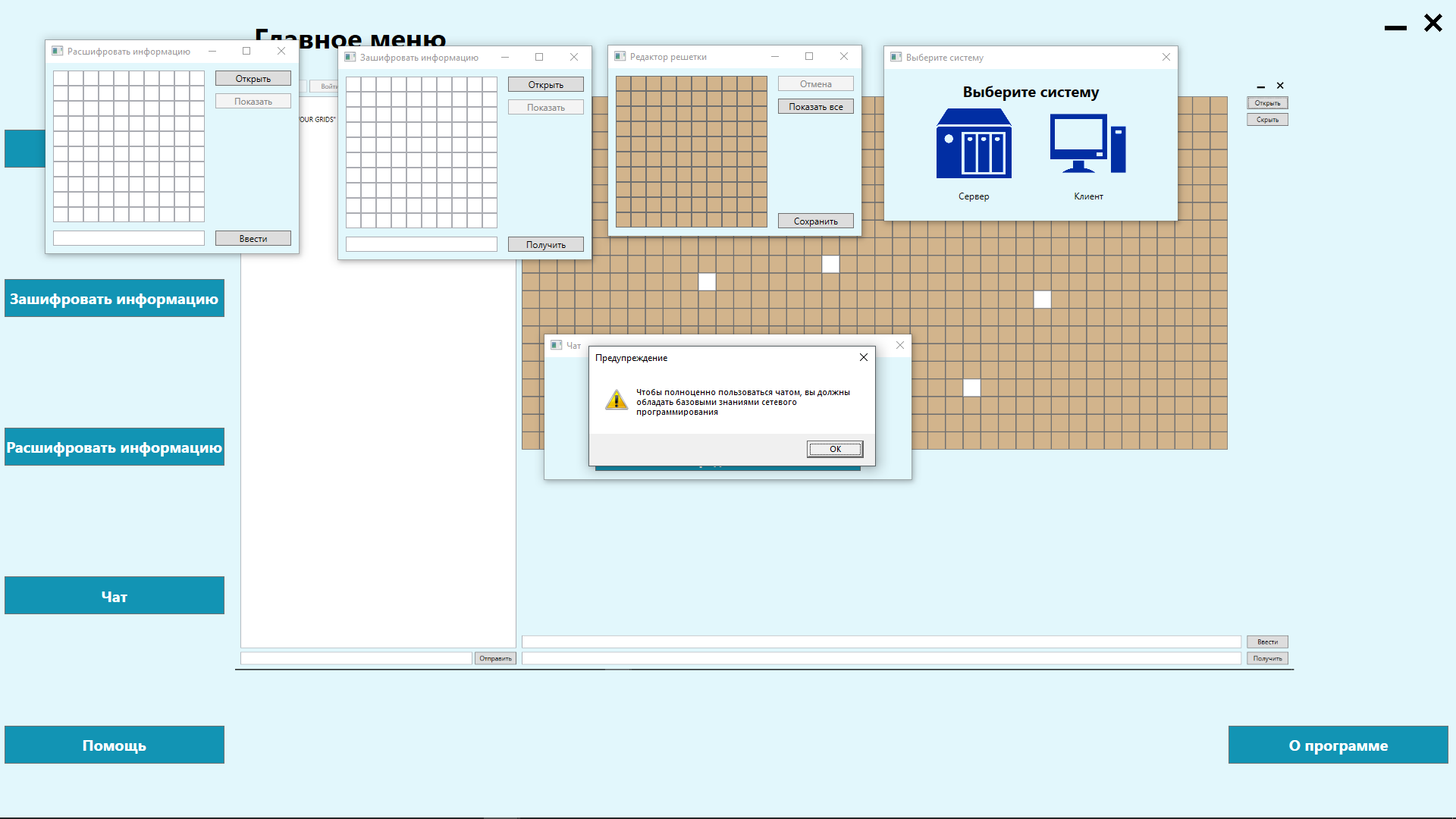


Рисунок 6. GrillEditor

Рисунок 5. InformationCoder

Рисунок 4. InformationDecoder

Рисунок 7. MessageBoxWarnnig

Рисунок 8. ServerOrClient

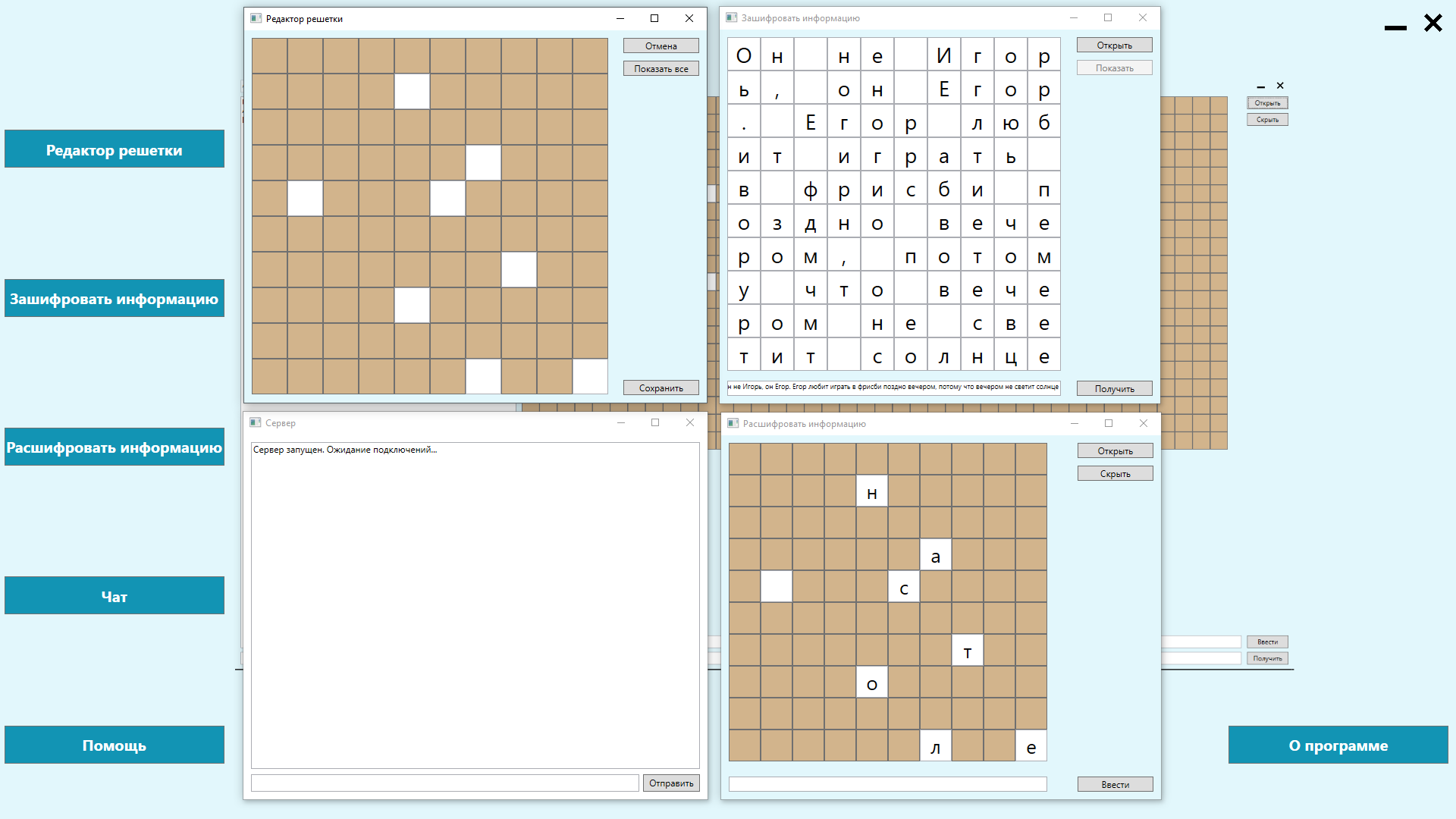
## 

## **3.2.1 Редактор решетки**

После того как пользователь запустил редактор решетки (рис. 6), ему следует нажать на те ячейки, которые он хочет оставить открытыми, затем нажать кнопку «Сохранить» и сохранить файл под каким-то именем в какой-либо директиве.

В окне присутствует кнопка отменить, которая отменяет последние действие пользователя. Так же существует кнопка, открывающая/закрывающая все ячейки.

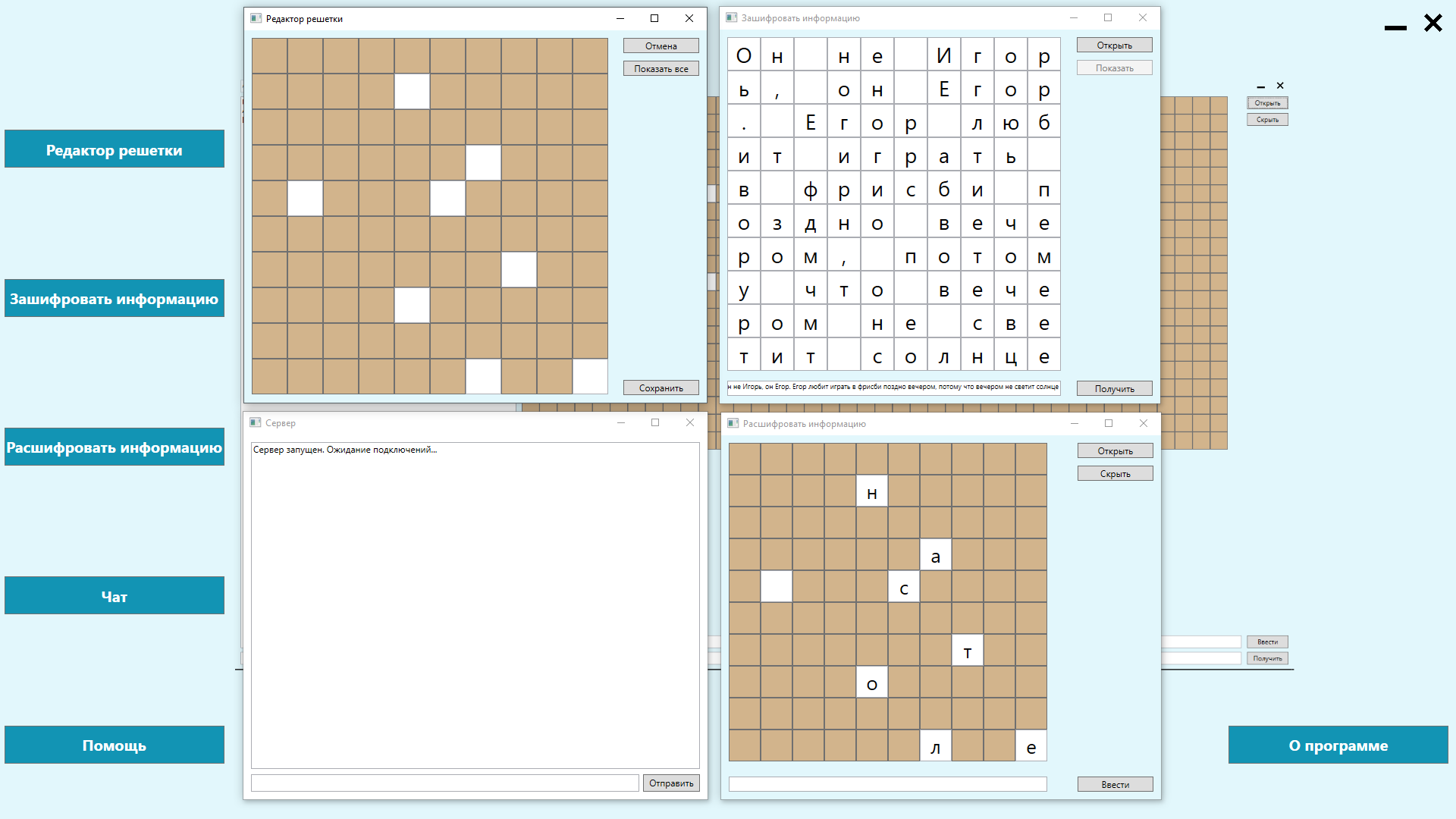
*Примерный результат работы приведен ниже*

**

## **3.2.2 Шифратор информации:**

После того как пользователь открыл шифратор информации, ему следует нажать на кнопку «Открыть» и открыть решетку, созданную в редакторе решетки, затем заполнить не закрытые ячейки информацией, которую необходимо зашифровать, затем скрыть решетку и заполнить оставшиеся пустые ячейки, после нажать кнопку получить и в нижней строке выведется зашифрованный текст. Полученный текст следует отправить другому пользователю, который имеет такую же решетку.

*Примерный результат работы приведен ниже*

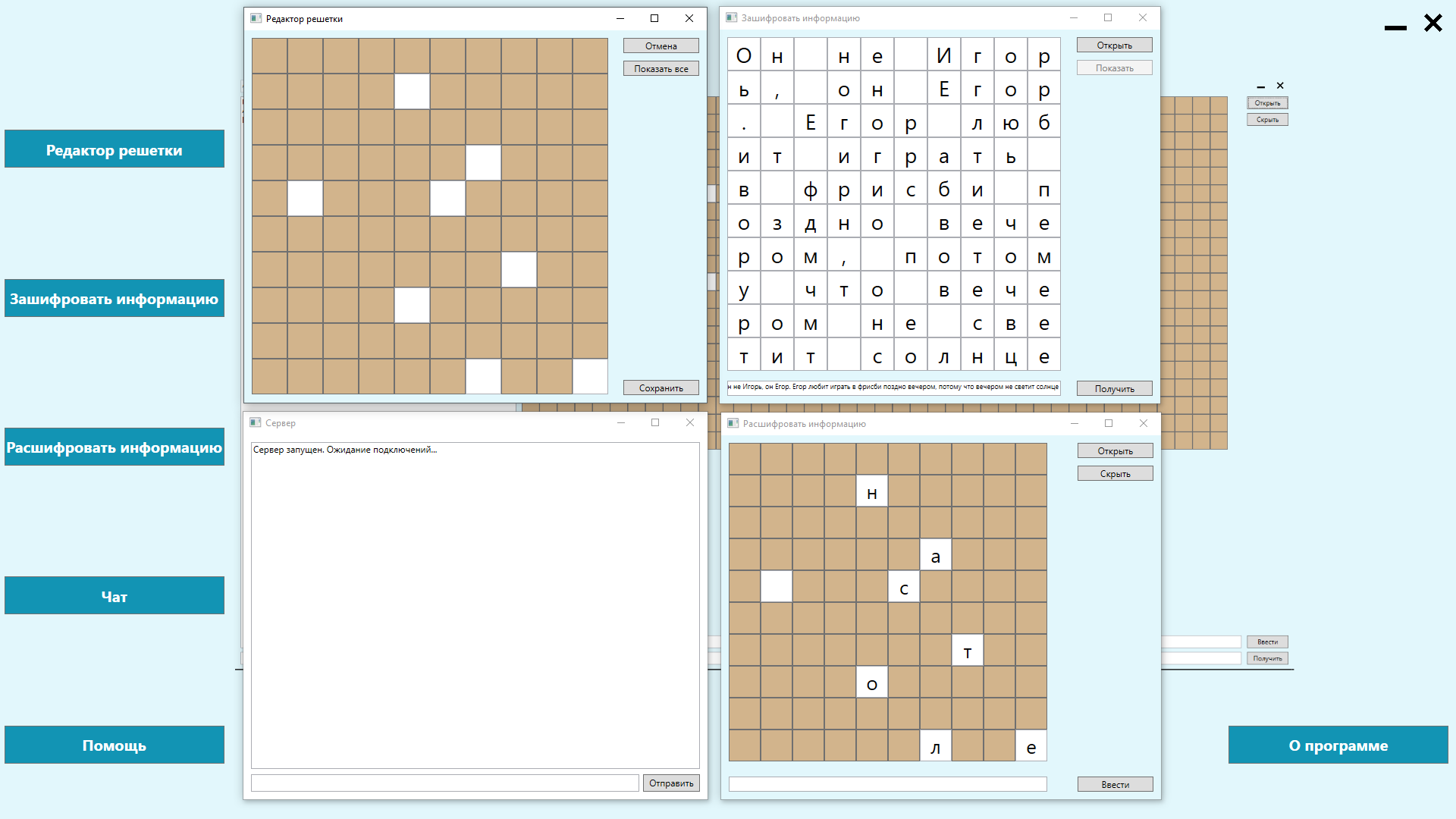


## **3.2.3 Дешифратор информации**

Для дешифрования информации необходим зашифрованный текст и решетка. Пользователю следует нажать на кнопку «Открыть», выбрать решетку для дешифрования, затем вставить в нижнее поле зашифрованный текст и нажать «Ввести». Открытые ячейки будут показывать текст, в той последовательности в которой его зашифровали.

Если решетка дешифрования совпадает с решеткой шифрования, то пользователь получит правильно расшифрованный текст.

*Примерный результат работы приведен ниже (способ чтения: слева направо, сверху вниз). Зашифрованный текст: «на столе»*

**

## **3.2.4 Чат**

После ввода размера решетки пользователю предоставляется выбор между чатом или клиентом (рис. 8). Чтобы запустить глобальный сервер пользователь должен быть уверен, что у него открыт порт для передачи данных на всех маршрутизаторах, ведущих к глобальной сети и узнать свой локальный ip (чтобы открыть порты необходимо зайти в настройки маршрутизатора, узнав адрес основного шлюза, чтобы узнать свой локальный ip необходимо запустить командную строку и ввести там «ipconfig» и нажать enter IPv4 является нужным для пользователя адресом). После выбора сервера необходимо ввести свой локальный ip и порт в соответствующие поля и нажать «Продолжить» (рис. 9), после нажать кнопку «Start» (рис. 10). Чтобы подключиться к серверу необходимо узнать глобальный ip сервера и порт, на котором запущен сервер, нажать соответствующий логотип в окне (рис. 8), ввести эти данные в соответствующие поля и нажать «Продолжить» (рис. 11). После запуска клиента в левом верхнем углу необходимо ввести свой никнейм и нажать кнопку «войти» (рис. 12). Если все данные были верны, то в чате появится надпись: «Подключен». Шифрование и дешифрование встроено в клиент и пользователь без проблем может шифровать и дешифровать сообщения, не открывая дополнительных окон и зная, как шифровать и дешифровать информацию.

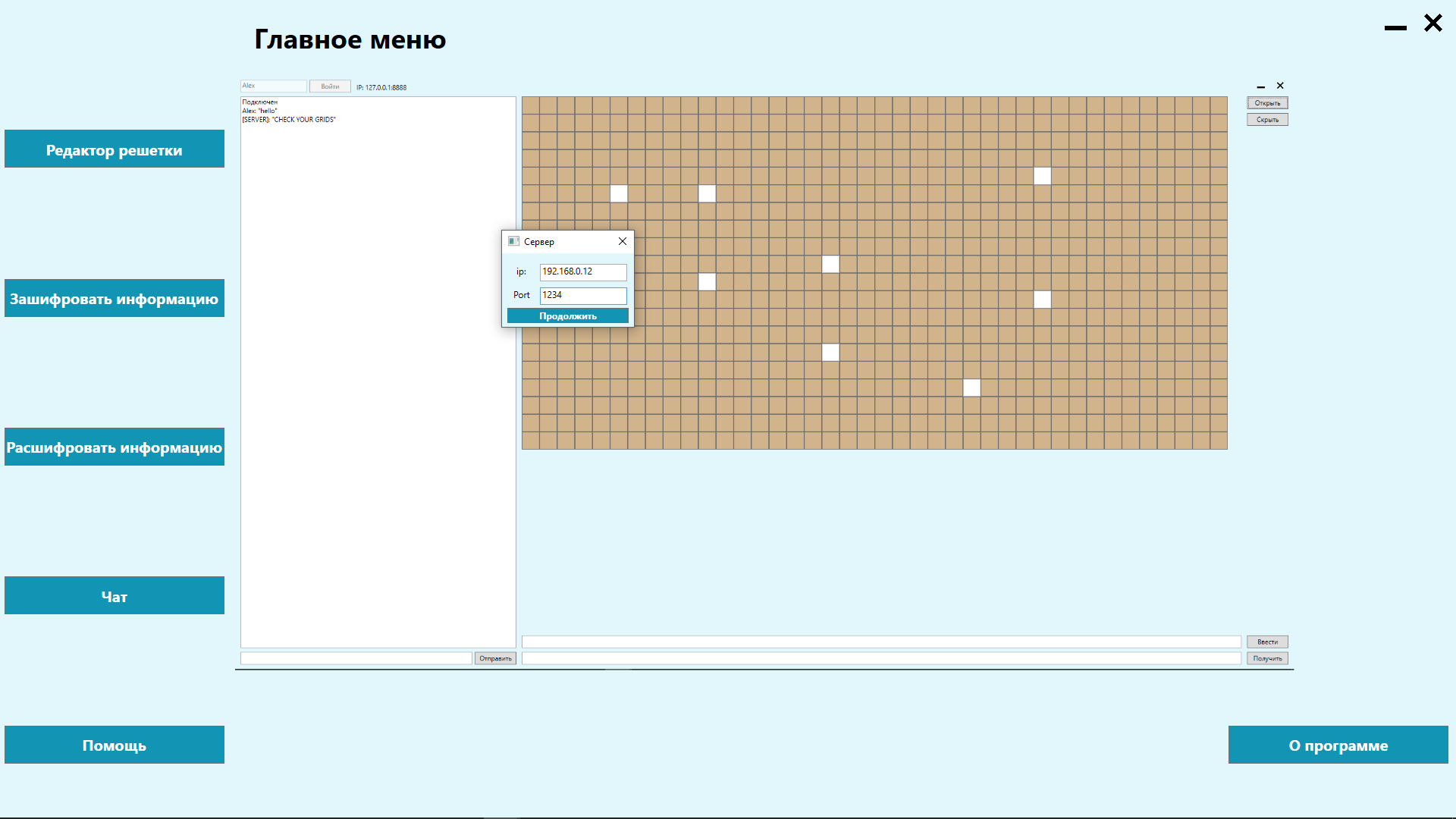
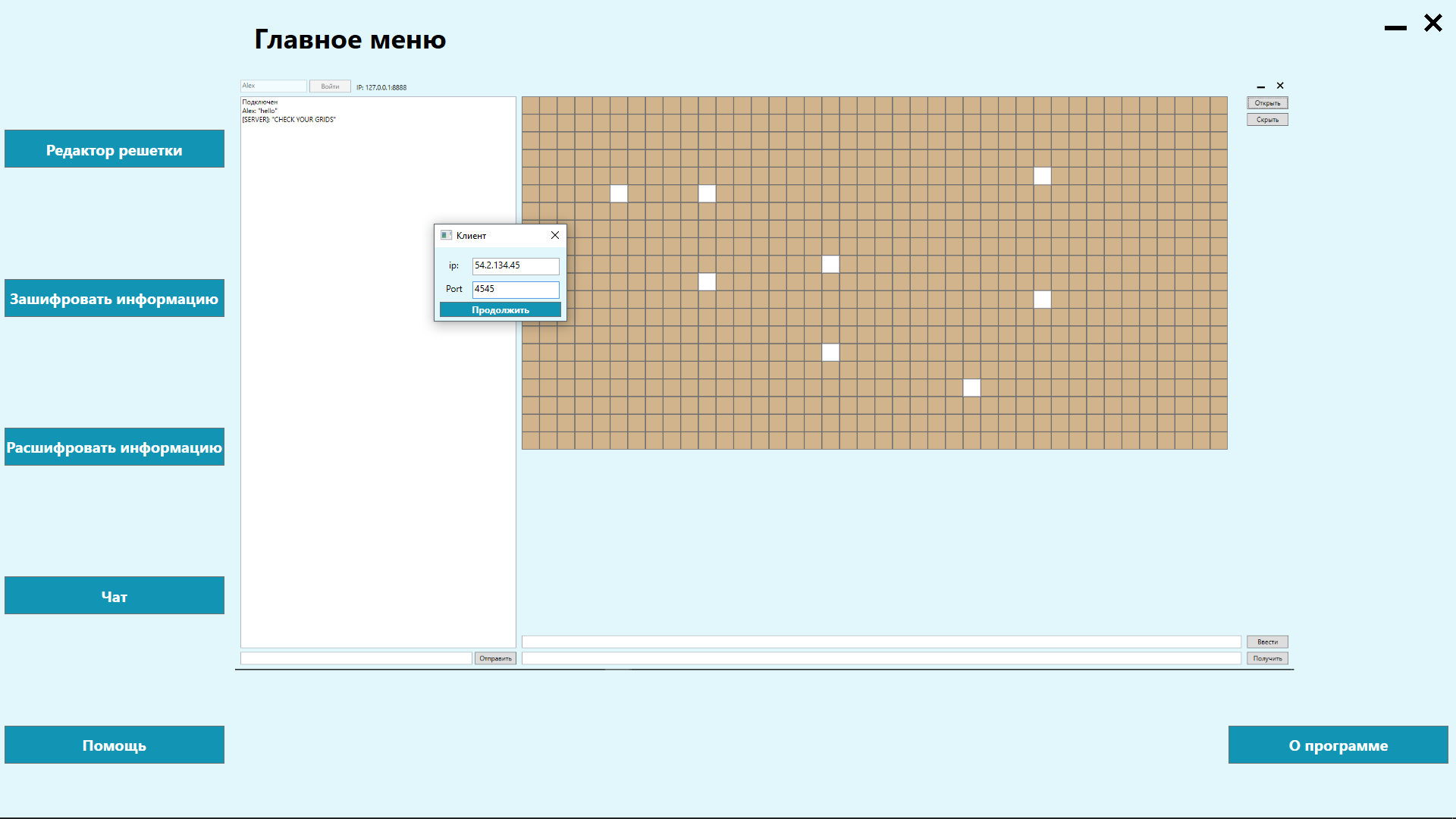
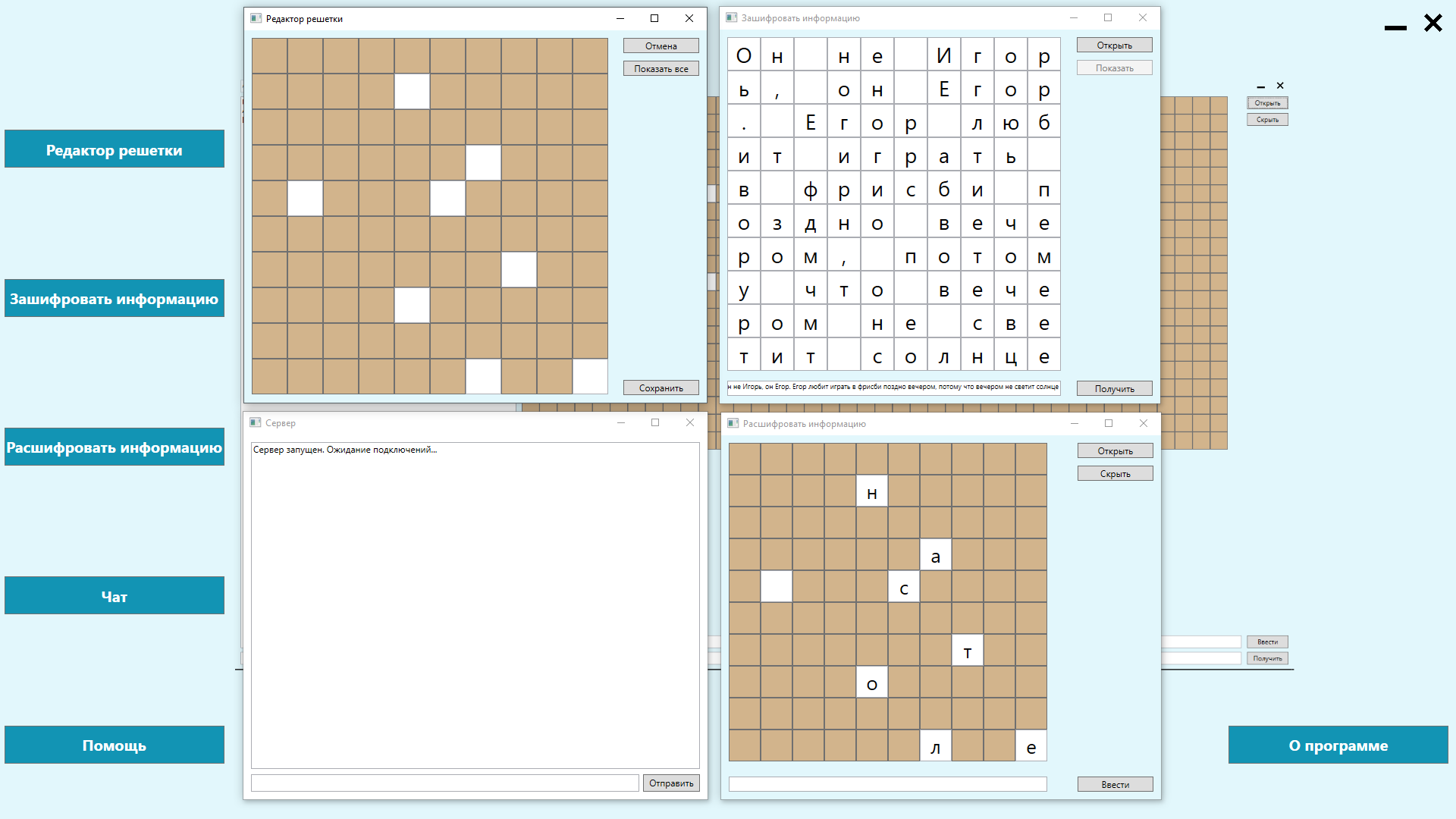


Рисунок 9. ServerAndClientSettings

Рисунок 11. ServerAndClientSettings

Рисунок 10. Server

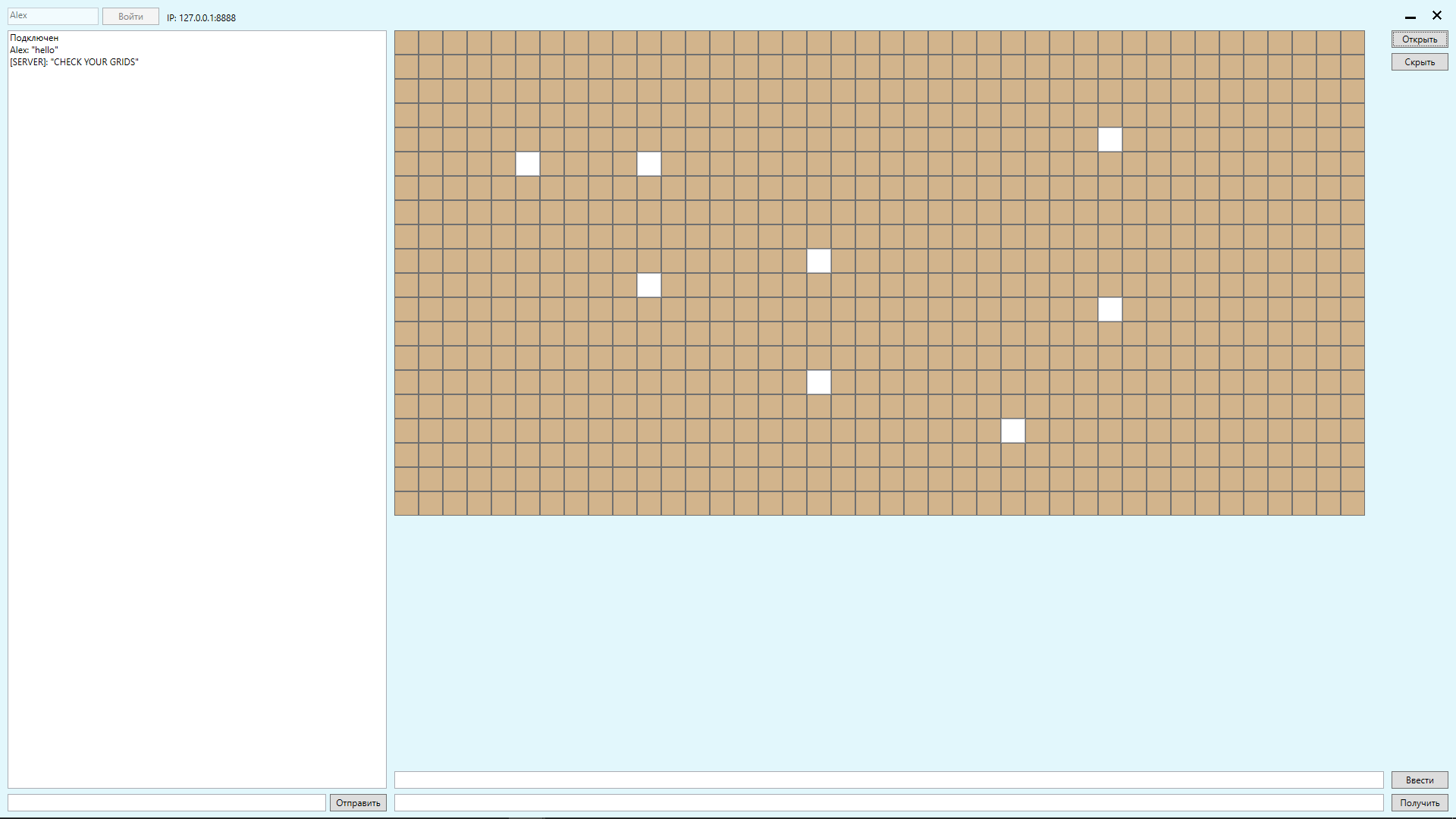


Рисунок 10. Client

## 

## **3.2.5 Помощь**

Когда пользователь нажимает на «Помощь», открывается окно, показывающее самую необходимую информацию о том, как нужно пользоваться программой (рис. 13).

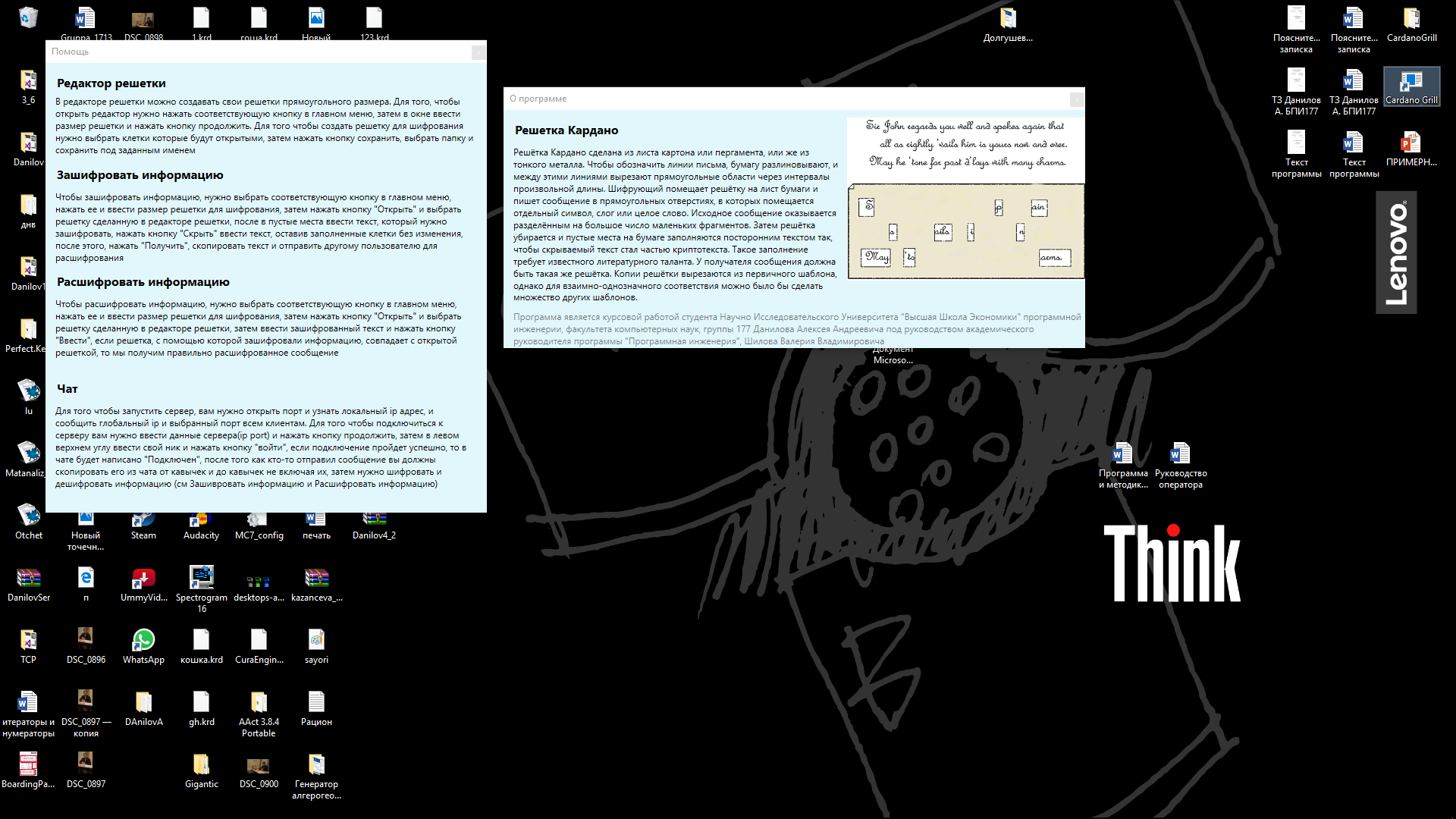


Рисунок 13. Help

## **3.2.6 О программе**

Когда пользователь нажимает на «О программе», открывается окно, показывающее краткую теорию и информацию об авторе (рис. 14).

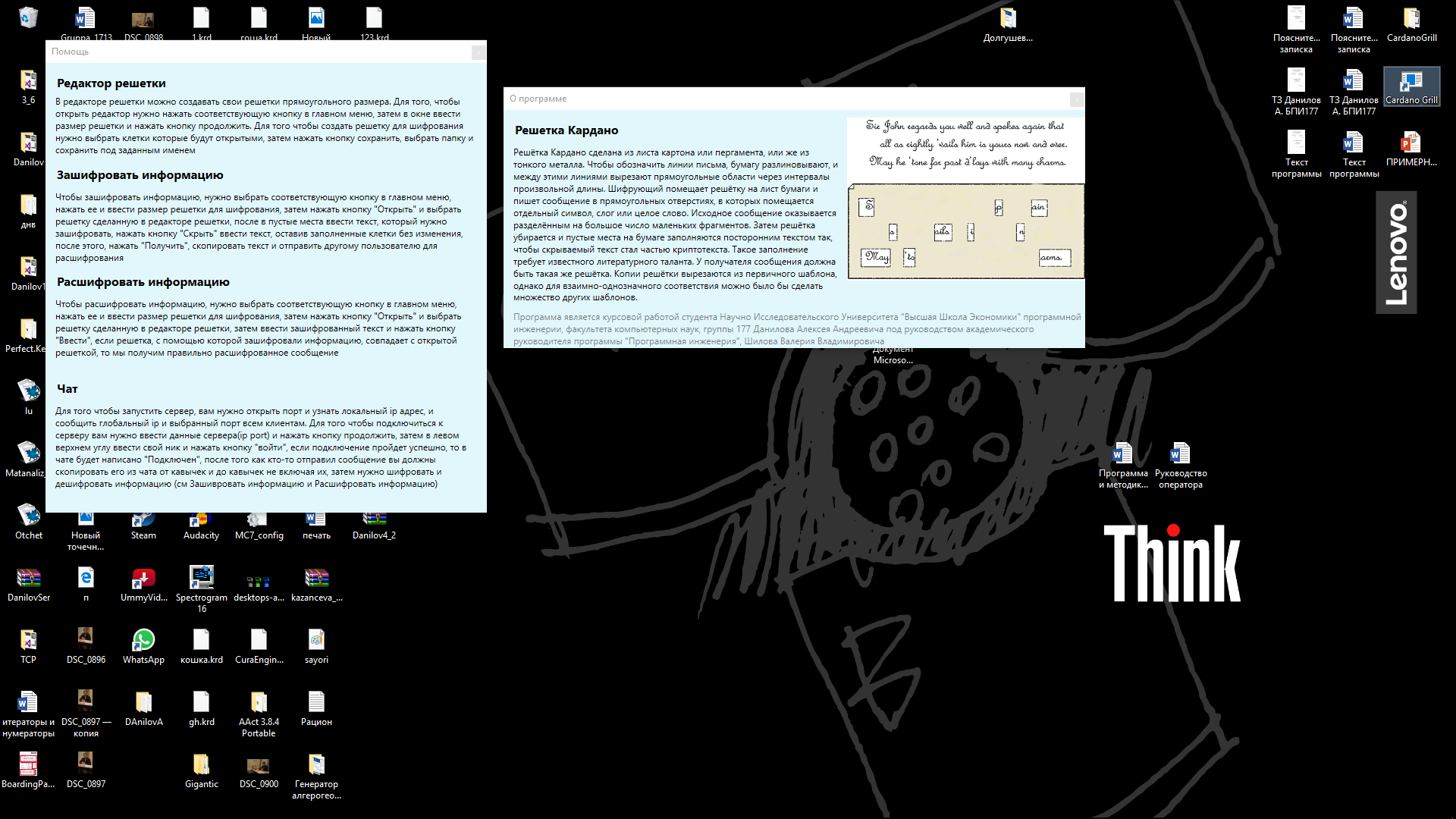


Рисунок 14. AboutProgramm

# **ПРИЛОЖЕНИЕ** **1**

**ТЕРМИНОЛОГИЯ**

|  |
| --- |
| Таблица 2 |

|  |  |
| --- | --- |
| **Термин** | **Определение** |
| **Решетка Кардано** | Инструмент шифрования и дешифрирования, представляющий собой специальную прямоугольную (в частном случае — квадратную) таблицу-карточку, часть ячеек которой вырезана. |
| **Шифрование** | Обратимое преобразование информации в целях скрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Шифрование служит для обеспечения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма. |

# **ПРИЛОЖЕНИЕ 2**

**ОПИСАНИЕ ФОРМАТА .krd**

Файл формата .krd содержит информацию о решетки, созданной в программе Cardano Grill, в текстовом виде.

Открыть файл формата .krd можно программой Cardano Grill.

Программа Cardano Grill при этом осуществляет корректное открытие только файлов формата .krd, созданных в этой программе.

# **ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Лист регистрации изменений | | | | | | | | | |
| Номера листов (страниц) | | | | | Всего листов (страниц в докум.) | № документа | Входящий № сопроводительного докум. и дата | Подп. | Дата |
| Изм. | Измененных | Замененных | Новых | Аннулированх |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |