**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 51 01-1** | | **ПРОГРАММА ДЛЯ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ**  **С ПОМОЩЬЮ РЕШЕТКИ КАРДАНО**  **Программа и методика испытаний**  **ЛИСТ УТВЕРЖДЕНИЯ**  **RU.17701729.5071102-01 51 01-1-ЛУ** | | |
|  |  | |
| Исполнитель:  студент группы БПИ177  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Данилов А.А. /  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. | |
|  | | |
|  | |  |

**2018**

|  |  |  |
| --- | --- | --- |
| **УТВЕРЖДЕНО**  **RU.17701729.5071102-01 51 01-1-ЛУ** |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл*** | **RU.17701729.5071102-01 51 01-1** | | **ПРОГРАММА ДЛЯ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ**  **С ПОМОЩЬЮ РЕШЕТКИ КАРДАНО**  **Программа и методика испытаний**  **RU.17701729.5071102-01 51 01-1**  **Листов 17** |
|
|
|  |  |
|  | **2018** |

Оглавление

[Аннотация 3](#_Toc514840048)

[**1. Объект испытаний** 5](#_Toc514840049)

[**2. Цель испытаний** 5](#_Toc514840050)

[**3. Требования к программе** 5](#_Toc514840051)

[**3.1.1** **Основные функции:** 5](#_Toc514840052)

[**3.1.2** **Дополнительные функции:** 5](#_Toc514840053)

[**4. Требования к программной документации** 6](#_Toc514840054)

[**5. Средства и порядок испытаний** 6](#_Toc514840055)

[**5.1 Технические средства** 6](#_Toc514840056)

[**5.2 Программные средства** 6](#_Toc514840057)

[**5.3 Порядок проведения испытаний** 7](#_Toc514840058)

[**6. Методы испытаний** 7](#_Toc514840059)

[**6.1 Испытания функциональности программы** 7](#_Toc514840060)

[**Основные функции:** 7](#_Toc514840061)

[**Дополнительные функции:** 12](#_Toc514840062)

[ПРИЛОЖЕНИЕ 1 13](#_Toc514840063)

[**ПРИЛОЖЕНИЕ 2** 14](#_Toc514840064)

[**ПРИЛОЖЕНИЕ 3** 15](#_Toc514840065)

[**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ** 15](#_Toc514840066)

Аннотация

Программа и методика испытаний – это документ, в котором содержится информация о программном продукте, а также полное описание приемочных испытаний для данного программного продукта.

Настоящая Программа и методика испытаний для «Программа для шифрования и дешифрования с помощью решетки Кардано» содержит следующие разделы: «Объект испытаний», «Цель испытаний», «Требования к программе», «Требования к программной документации», «Средства и порядок испытаний», «Приложения» [7].

В разделе «Объект испытаний» указано наименование и область применения программы.

В разделе «Цель испытаний» указана цель проведения испытаний. Раздел «Требования к программе» содержит основные требования к программе, которые подлежат проверке во время испытаний.

Раздел «Требования к программным документам» содержит состав программной документации, которая представляется на испытания.

Раздел «Средства и порядок испытаний» содержит информацию о технических и программных средствах, которые следует использовать во время испытаний, а также порядок этих испытаний.

Раздел «Методы испытаний» содержит информацию об используемых методах испытаний.

Настоящий документ разработан в соответствии с требованиями:

1) ГОСТ 19.101-77 Виды программ и программных документов [1];

2) ГОСТ 19.102-77 Стадии разработки [2];

3) ГОСТ 19.103-77 Обозначения программ и программных документов [3];

4) ГОСТ 19.104-78 Основные надписи [4];

5) ГОСТ 19.105-78 Общие требования к программным документам [5];

6) ГОСТ 19.106-78 Требования к программным документам, выполненным печатным способом [6];

7) ГОСТ 19.301-79 Программа и методика испытаний. Требования к содержанию и оформлению [7].

Изменения к данному документу оформляются согласно ГОСТ 19.603-78 [8], ГОСТ 19.604-78 [9].

Перед прочтением данного документа рекомендуется ознакомиться с терминологией, приведенной в Приложении 1 настоящей программы и методики испытаний.

# **1. Объект испытаний**

**Наименование:** «Программа для шифрования и дешифрования с помощью решетки Кардано».

**Краткая характеристика и область назначения:** «Программа для шифрования и дешифрирования с помощью решетки Кардано» – прикладная программа, позволяющая шифровать и дешифрировать сообщения с помощью решетки Кардано и общаться с помощью зашифрованных сообщений по сети.

# **2. Цель испытаний**

Целью испытаний является проверка корректности выполнения программой функций, перечисленных в разделе «Требования к программе».

# **3. Требования к программе**

Программа должна соответствовать следующим функциональным требованиям, указанным в документе «Программа для шифрования и дешифрирования с помощью решетки Кардано. Техническое задание»:

* + 1. **Основные функции:**

1) Создание решетки Кардано;

2) Шифрование информации, вводимой пользователем;

3) Дешифрование информации, вводимой пользователем;

* + 1. **Дополнительные функции:**

1. Общение зашифрованными данными через Интернет-соединение;
2. Теоретическая справка.

# **4. Требования к программной документации**

На испытание должна быть представлена документация в следующем составе:

1. «Программа для шифрования и дешифрирования с помощью решетки Кардано». Техническое задание (ГОСТ 19.201-78);
2. «Программа для шифрования и дешифрирования с помощью решетки Кардано». Программа и методика испытаний (ГОСТ 19.301-78);
3. «Программа для шифрования и дешифрирования с помощью решетки Кардано». Пояснительная записка (ГОСТ 19.404-79);
4. «Программа для шифрования и дешифрирования с помощью решетки Кардано». Руководство оператора (ГОСТ 19.505-79).
5. «Программа для шифрования и дешифрирования с помощью решетки Кардано». Текст программы (ГОСТ 19.401-78);

# **5. Средства и порядок испытаний**

## **5.1 Технические средства**

Во время испытаний должны быть использованы следующие технические средства:

1) операционная система Microsoft Windows XP SP3 или более поздняя версия;

2) установленный Microsoft .NET Framework 3.5, требующий Windows Installer 3.1 или более поздняя версия;

3) Internet Explorer 6.0 или более поздняя версия.

Для работы программы необходим следующий состав технических средств:

1) персональный компьютер, оснащенный 32-разрядным (x86) или 64-разрядным (x64) процессором Pentium с тактовой частотой 400 MГц и выше или аналогичный процессор (рекомендуется Pentium с тактовой частотой 1 ГГц и выше или аналогичный процессор);

2) 96 МБ оперативной памяти или больше (рекомендуется 256 МБ оперативной памяти или больше);

3) не менее 1,5 ГБ свободного места на жестком диске;

4) видеокарта и монитор, поддерживающие режим Super VGA с разрешением не менее чем 1000x600 точек;

5) мышь Microsoft Mouse или совместимое указывающее устройство;

6) клавиатура;

## **5.2 Программные средства**

Во время испытаний должны быть использованы следующие программные средства:

1) операционная система Microsoft Windows 7 или более поздняя версия;

2) последняя версия драйвера видеокарты.

## **5.3 Порядок проведения испытаний**

Испытания должны проводиться в следующем порядке:

1. Выполнить стандартную процедуру начальной загрузки операционной системы.

2. Вставить в компьютер информационный накопитель, содержащий программный продукт.

3. Скопировать папку “ Программа для шифрования и дешифрования с помощью решетки Кардано” на компьютер, на котором проводятся испытания.

4. Запустить программу двойным щелчком по файлу Cardano Grill.exe.

5. Провести испытания, описанные ниже в разделе «Методы испытаний».

6. Выйти из программы.

# **6. Методы испытаний**

Испытания представляют собой процесс установления соответствия программы заданным требованиям и программной документации.

Основной интерфейс программы состоит из шести окон: MainWindow, GrillEditor, InfformationCoder, InformationDecoder, Client и Server.

## **6.1 Испытания функциональности программы**

Функционал программы проверяется в соответствии с указанными в документе «Программа для шифрования и дешифрирования с помощью решетки Кардано. Техническое задание»:

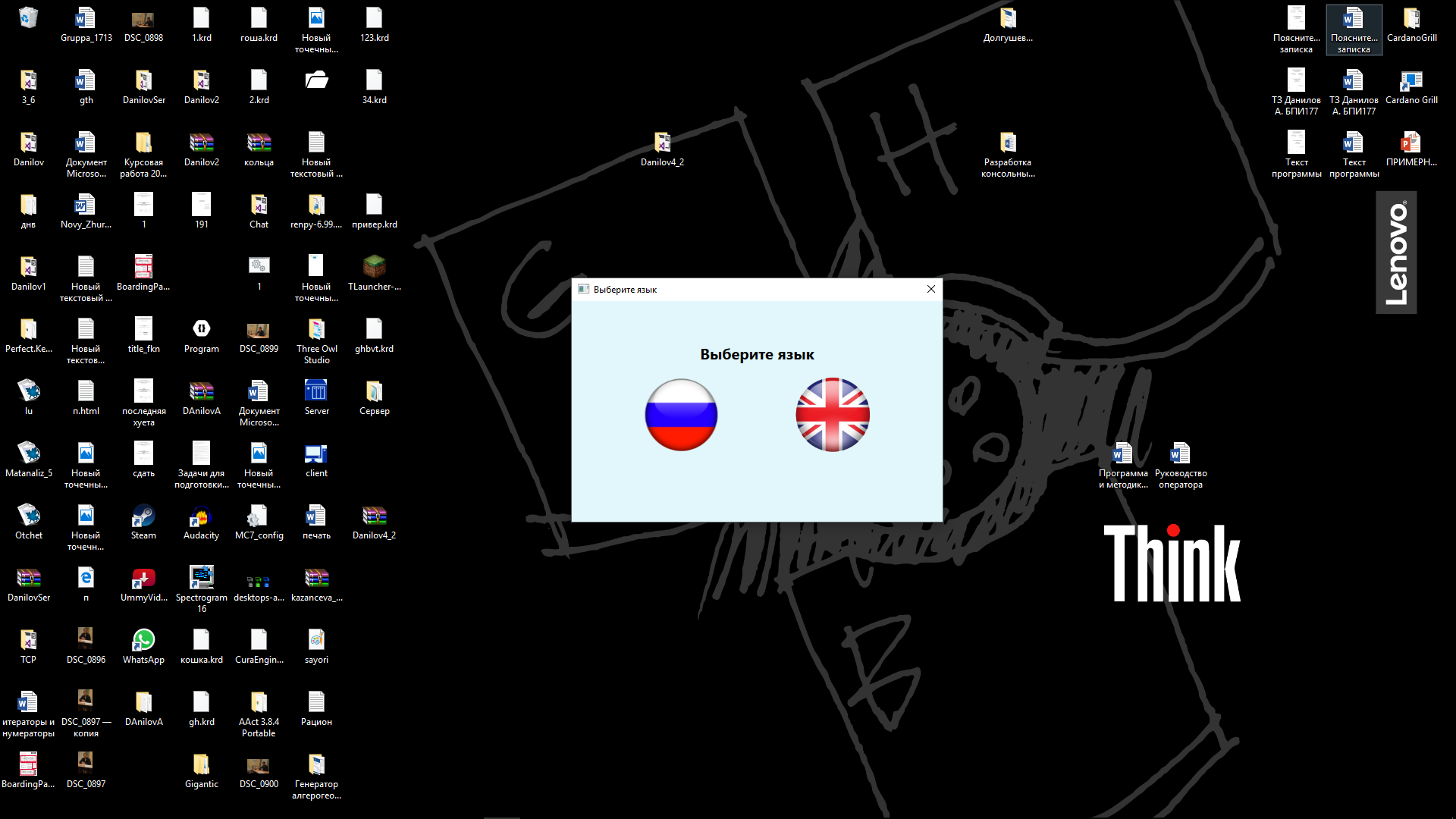


Рисунок .MainWindow

**Основные функции:**

1. Создание решетки Кардано.

Запускаем приложение (рис.1). Для входа в главное меню необходимо выбрать язык.

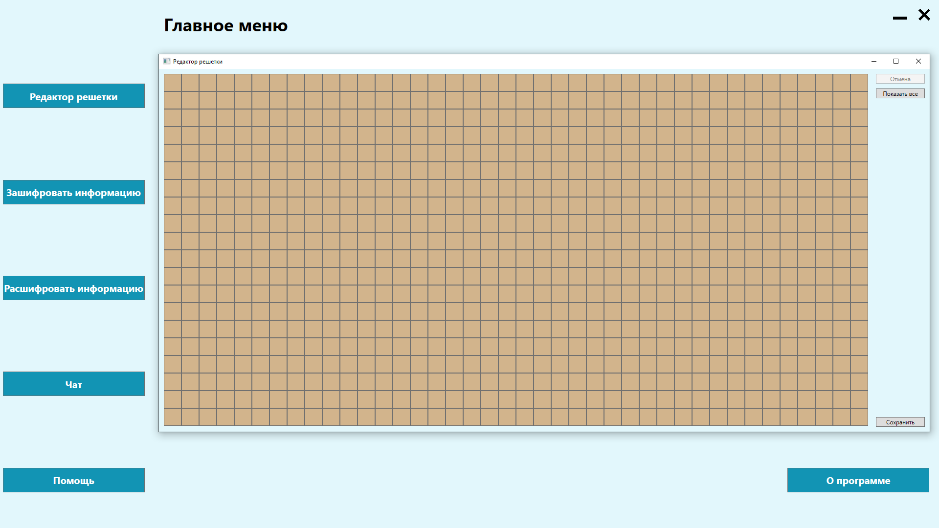
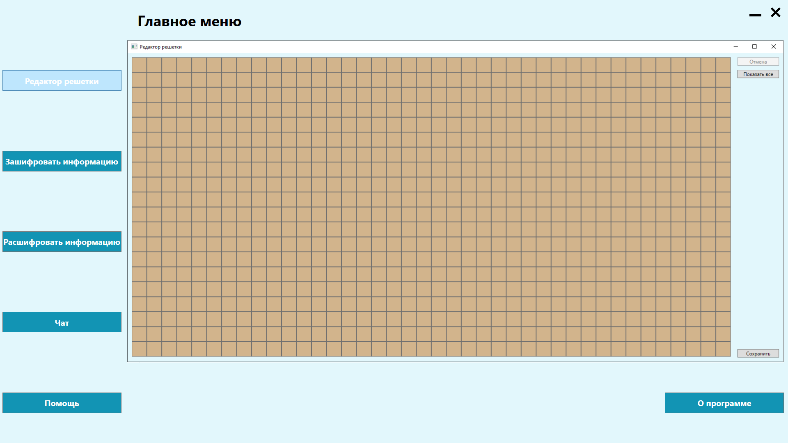
Переходим к окну MainMenu (рис. 2) и нажимаем на кнопку «Редактор решетки» (рис. 3).

Рисунок . MainMenu

Рисунок .MainMenu

Рисунок .EnteringField

В открывшемся окне EnteringField (рис. 4) вводим высоту и ширину решетки и переходим по кнопке «Продолжить» (если пользователь ввел неверные данные, появляется сообщение (рис. 5)).

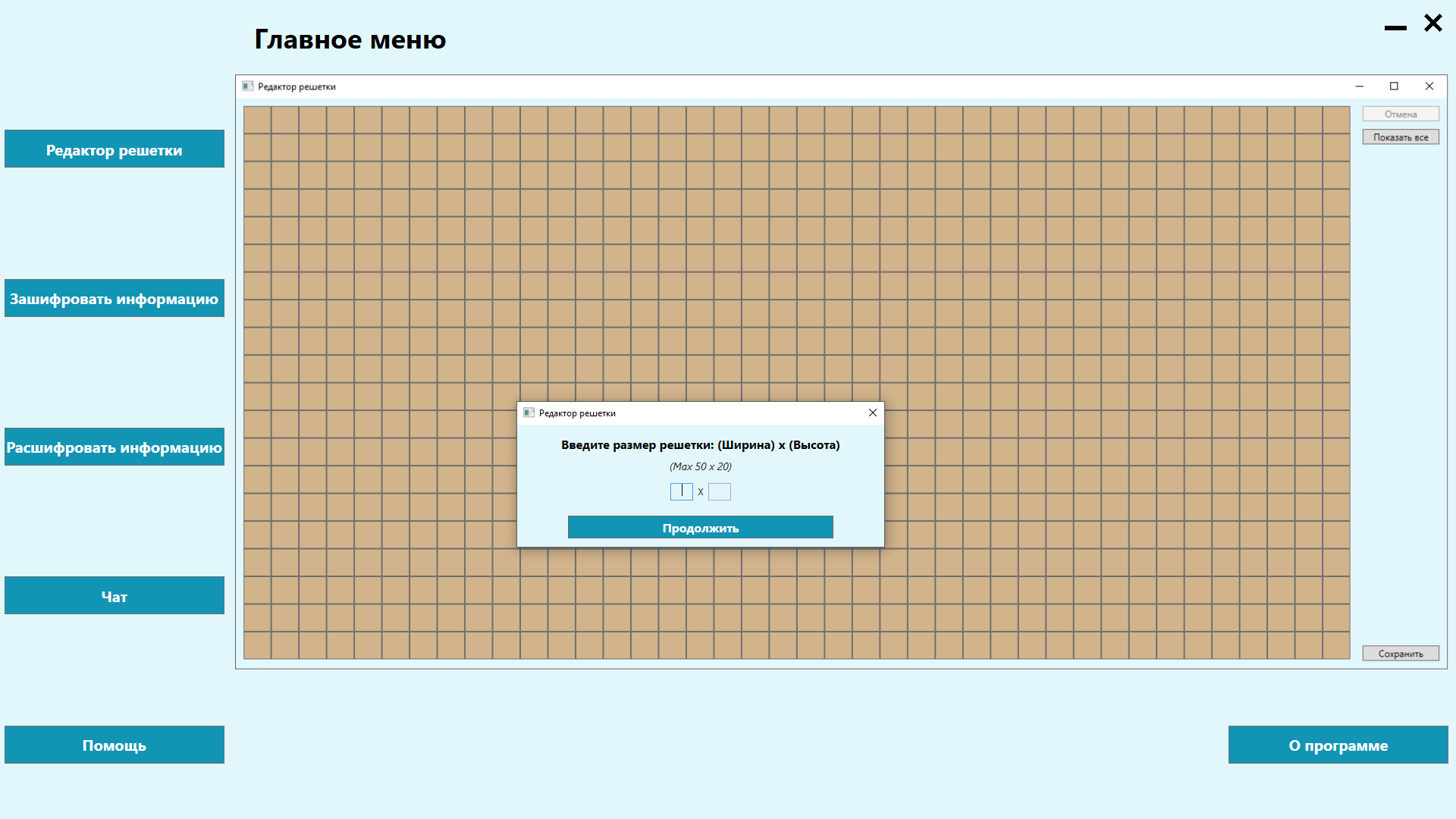
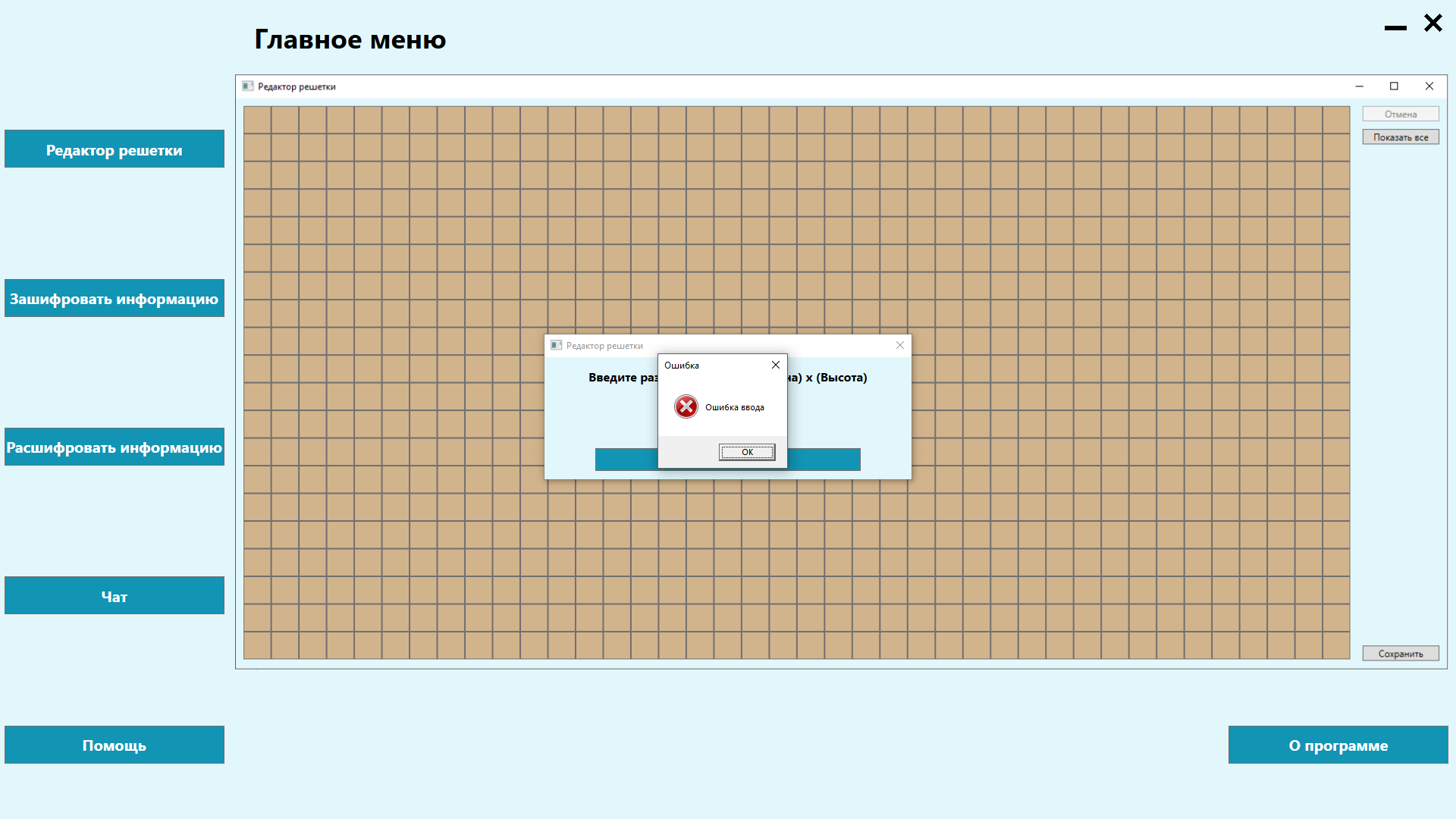


Рисунок 5. CodeGeneratingWindow

После того, как пользователь запустил редактор решетки (рис. 6), ему доступен следующий функционал:

1. Нажатие на ячейку открывает ячейку (рис. 7)
2. Нажатие на «Отмена» отменяет последнее действие (рис. 8)
3. Нажатие на «Показать все» отображает все ячейки закрытыми (рис. 9)
4. Нажатие на «Скрыть все» отображает все ячейки открытыми (рис. 10)
5. Нажатие на «Сохранить» сохраняет файл (рис. 11)

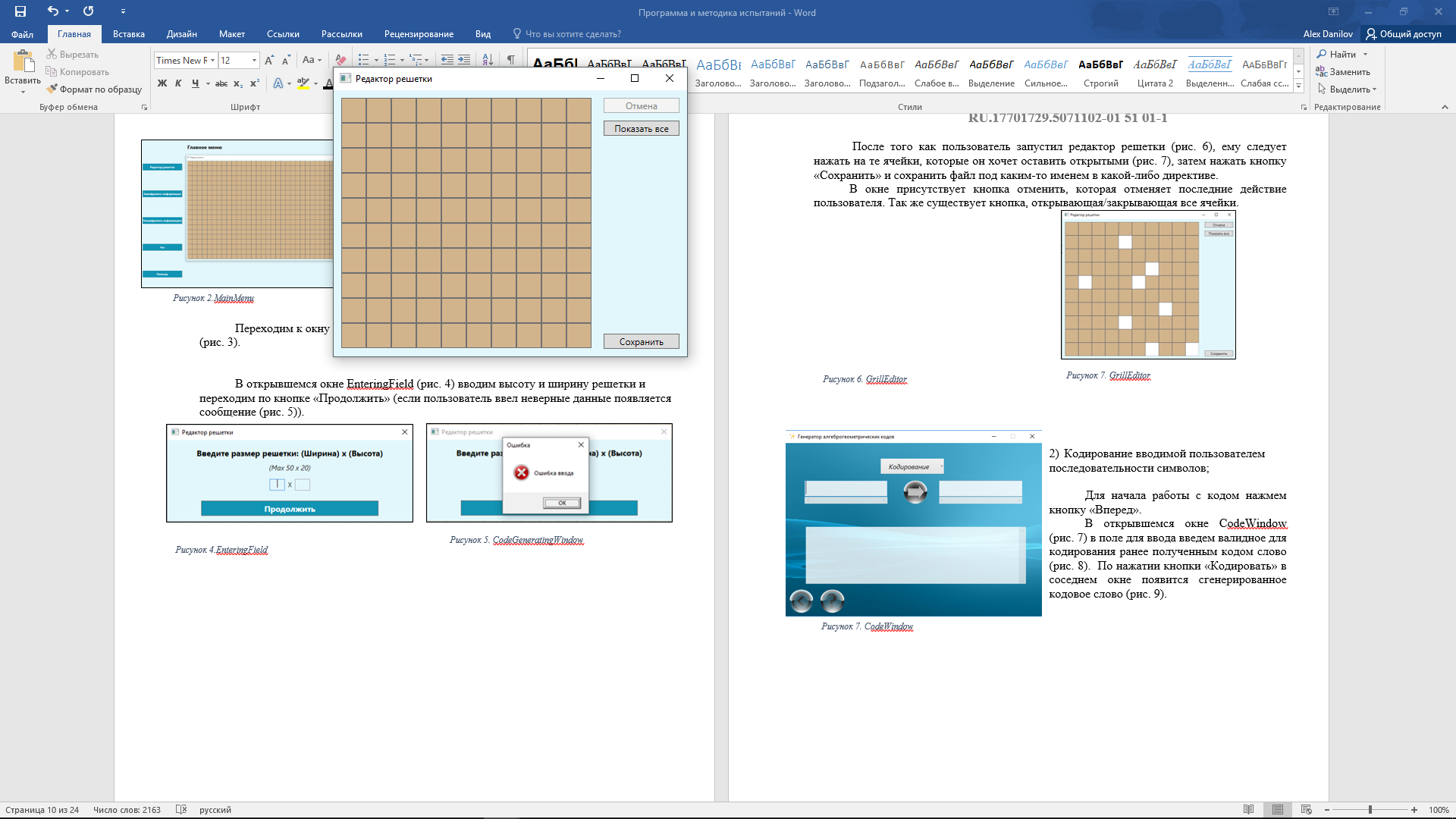
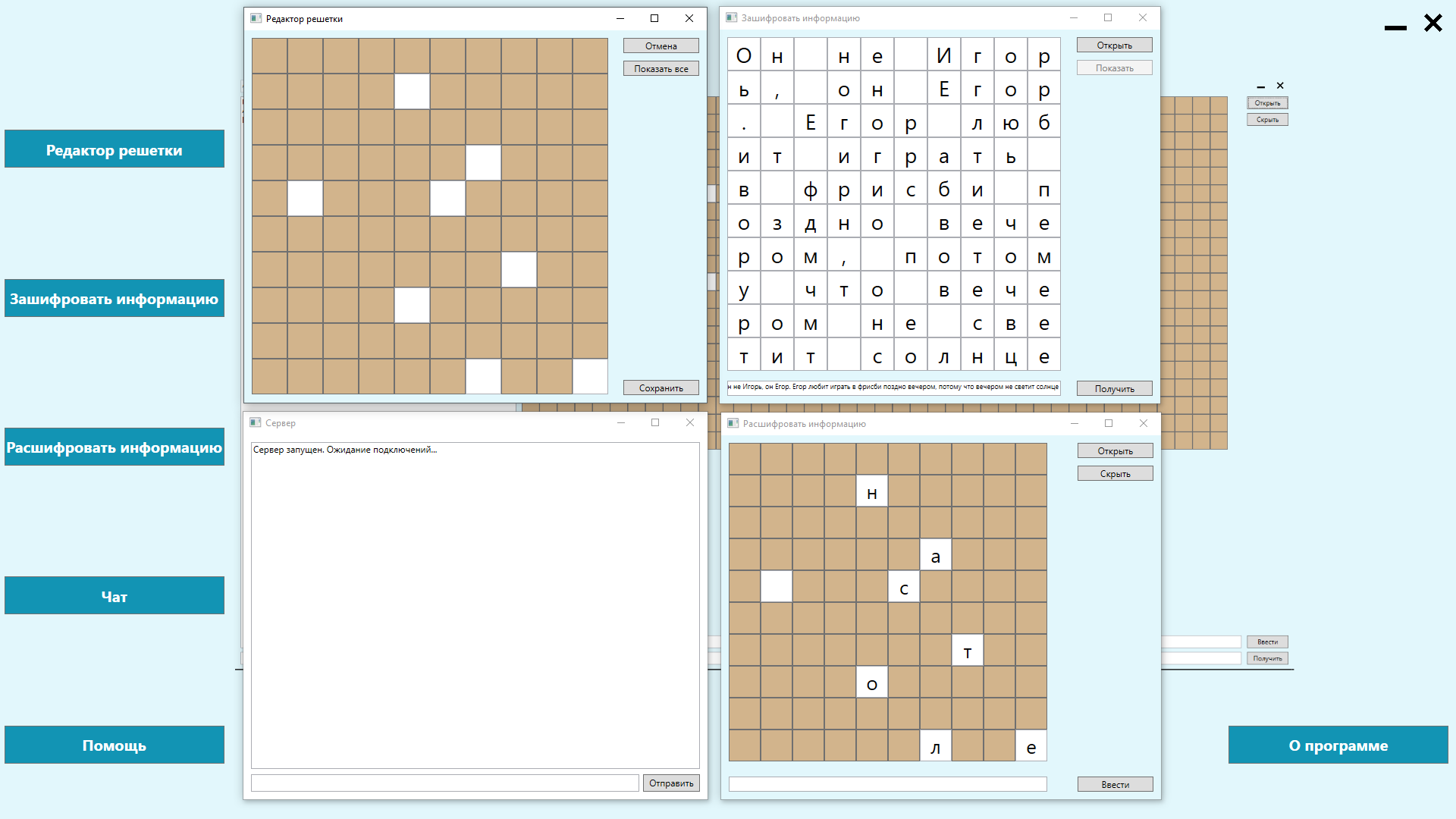
**

Рисунок 7. GrillEditor и нажатые ячейки

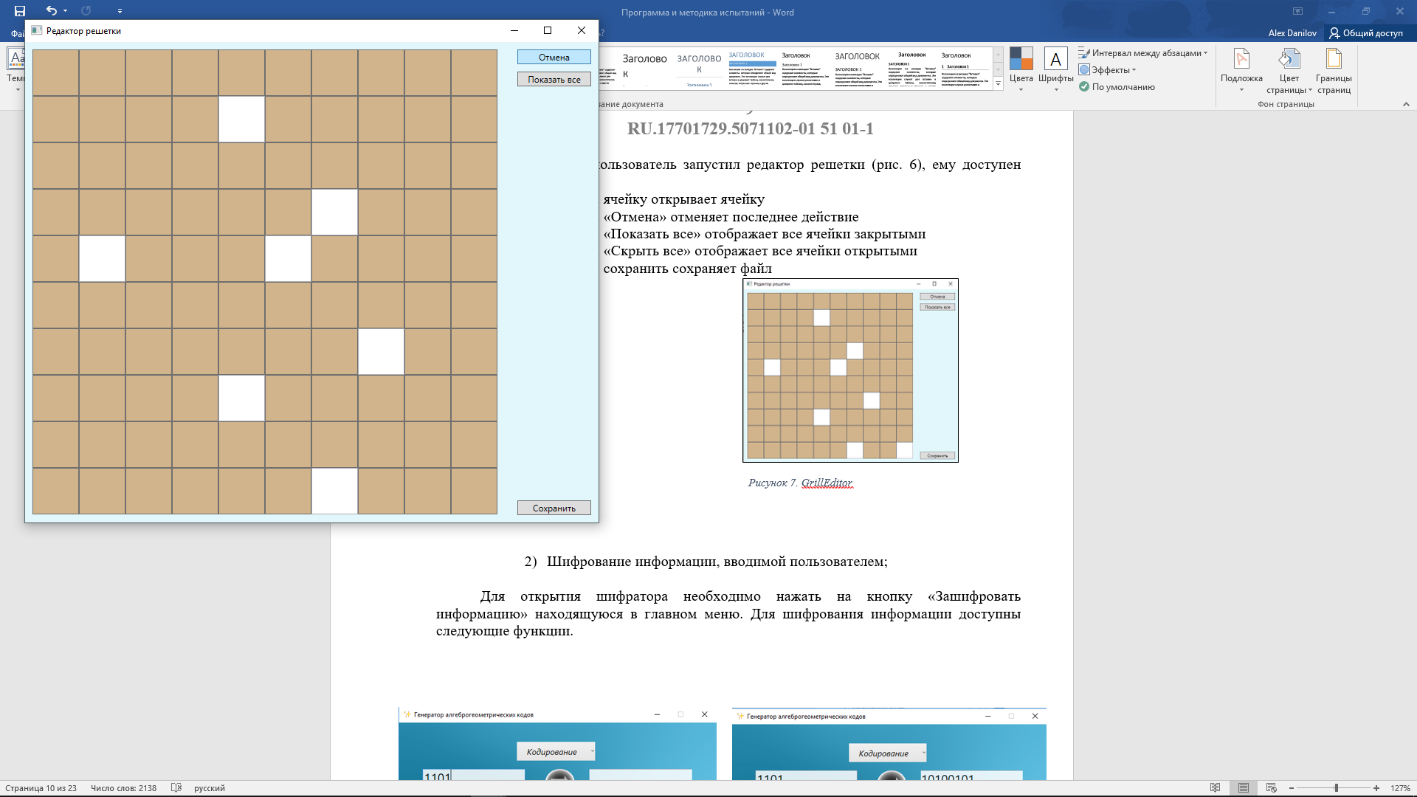
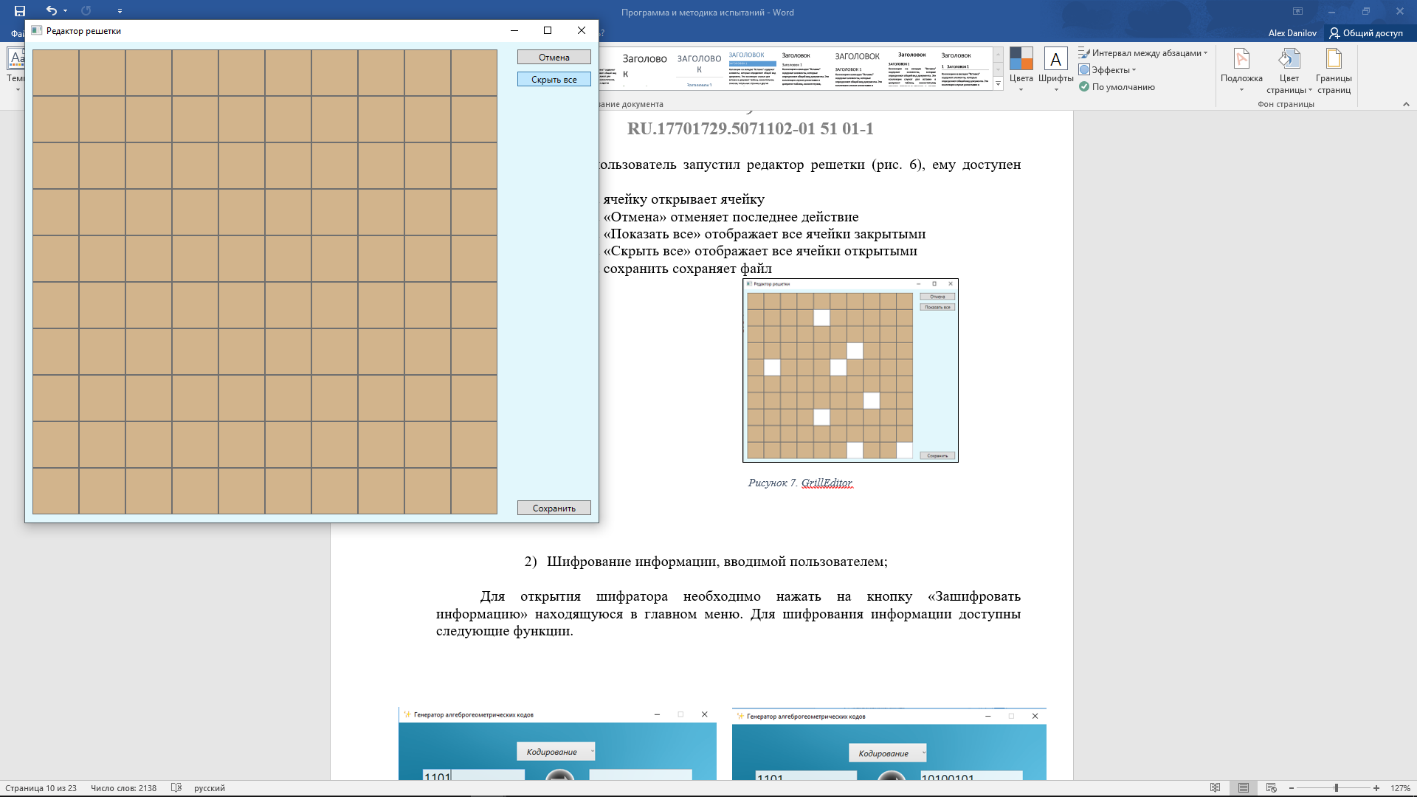


Рисунок 6. GrillEditor

Рисунок 9. GrillEditor и нажатие кнопки показать все

Рисунок 8. GrillEditor и нажатие кнопки отмена

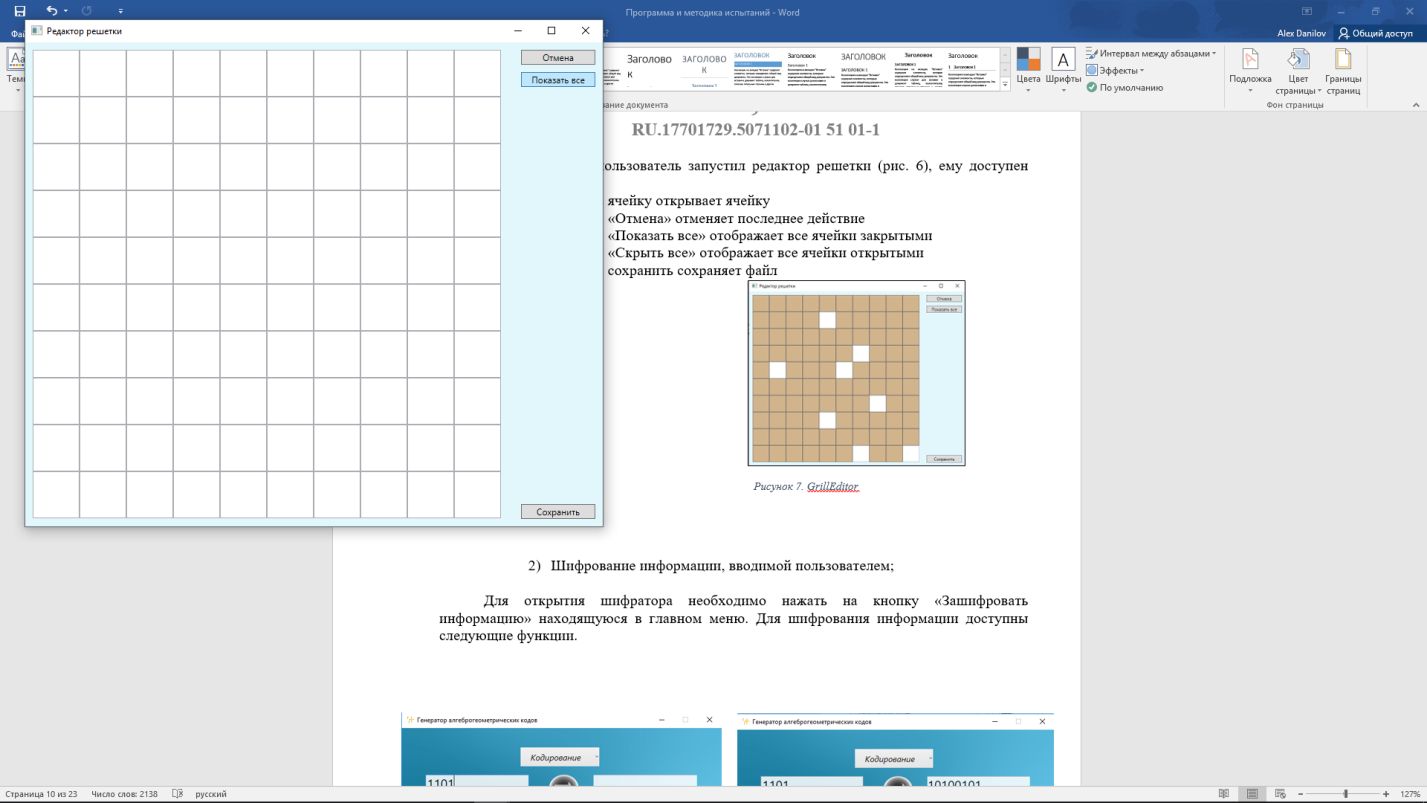




Рисунок 11. GrillEditor и нажатие кнопки скрыть все

Рисунок 10. GrillEditor и нажатие кнопки скрыть все

1. Шифрование информации, вводимой пользователем;

Для открытия шифратора необходимо нажать на кнопку «Зашифровать информацию», находящуюся в главном меню. Для шифрования информации доступны следующие функции (рис. 12).

1. Нажатие на кнопку «Открыть» позволяет выбрать решетку, которую необходимо открыть (рис. 13)
2. Нажатие на кнопку «Показать»/«Скрыть» показывает/скрывает решетку (рис. 14)
3. Нажатие на кнопку получить выдает зашифрованную строку (рис. 15)

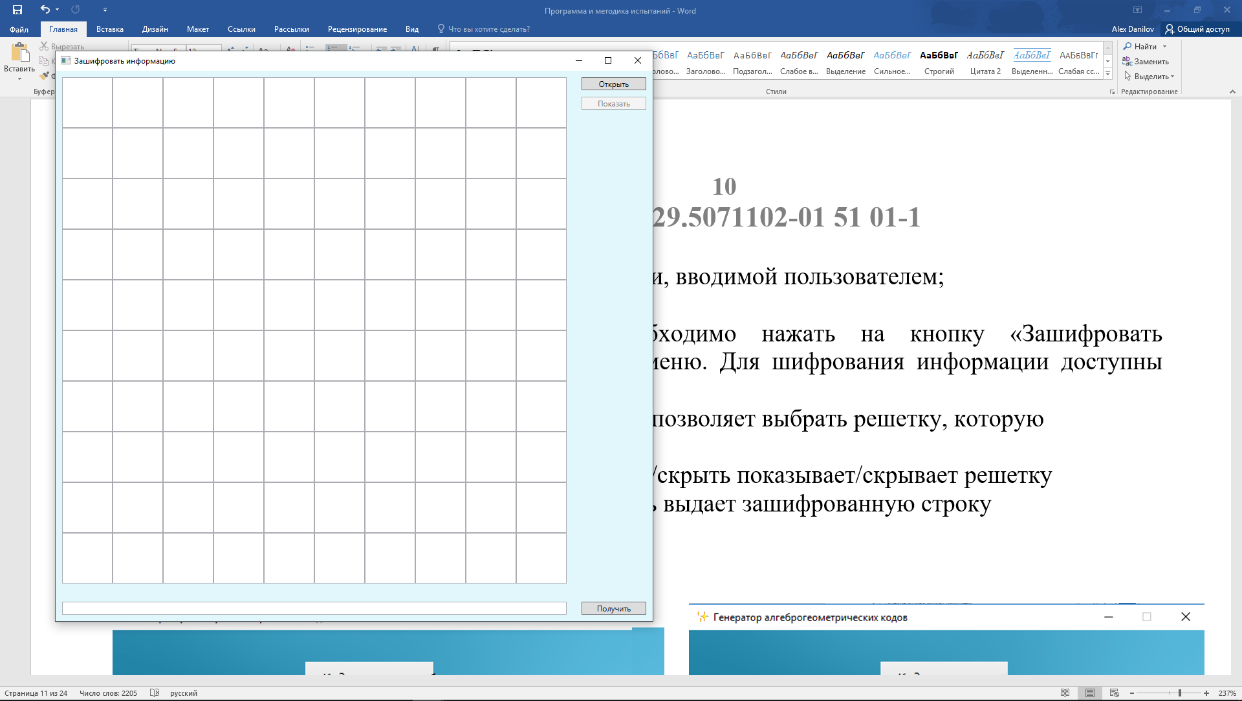
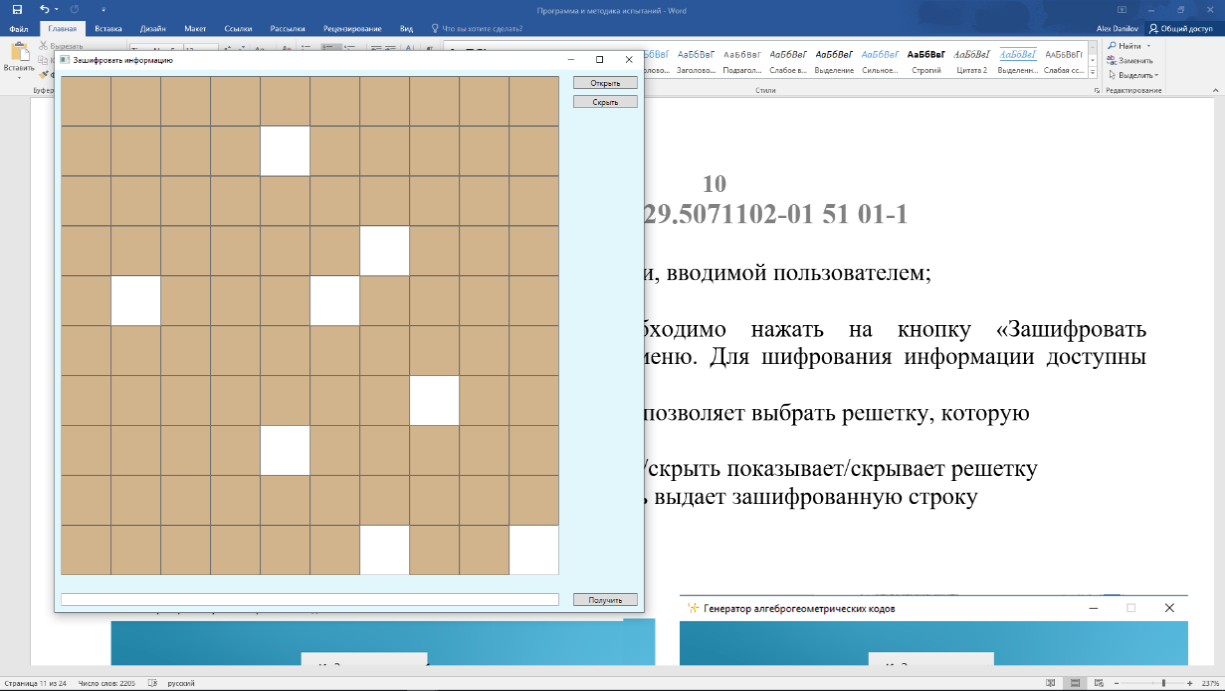


Рисунок 13. InformationCoder с открытой решеткой

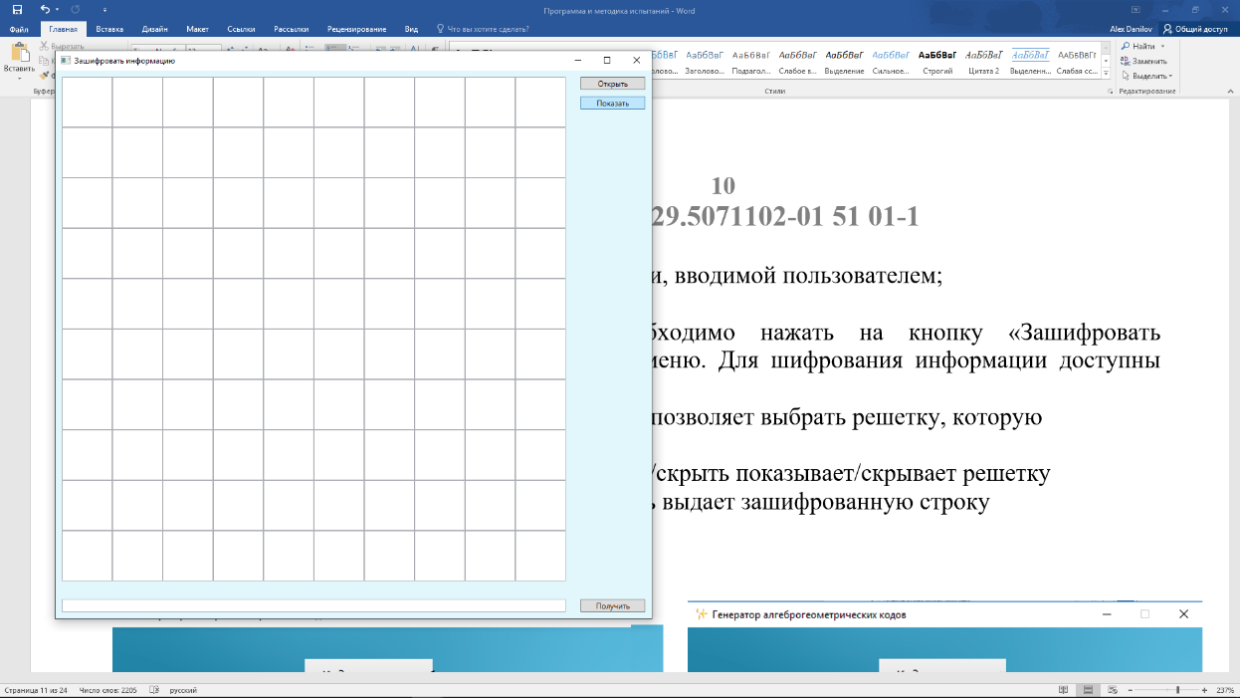
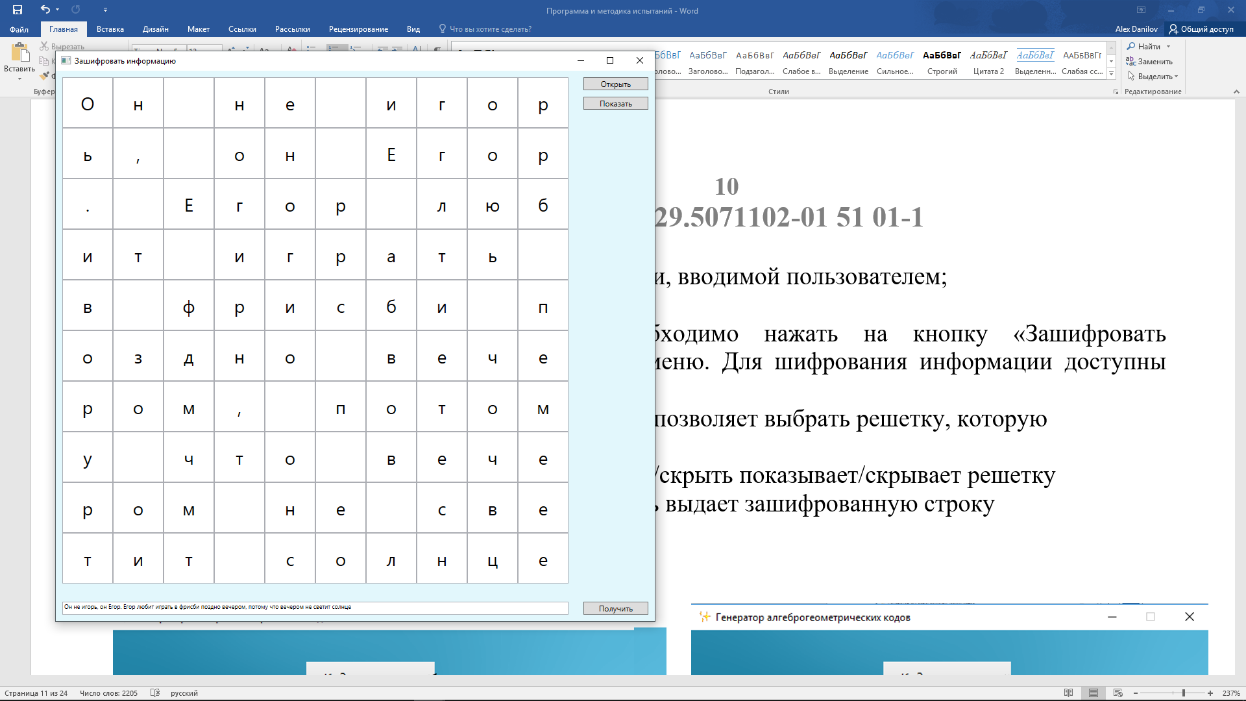


Рисунок 12. InformationCoder

Рисунок 15. InformationCoder нажатие кнопки получить

Рисунок 14. InformationCoder нажатие кнопки скрыть

1. Дешифрование абсолютно идентично шифрованию, только вместо кнопки «Получить» стоит кнопка «Ввести», которая запускает метод, вводящий текст в решетку (рис. 16)

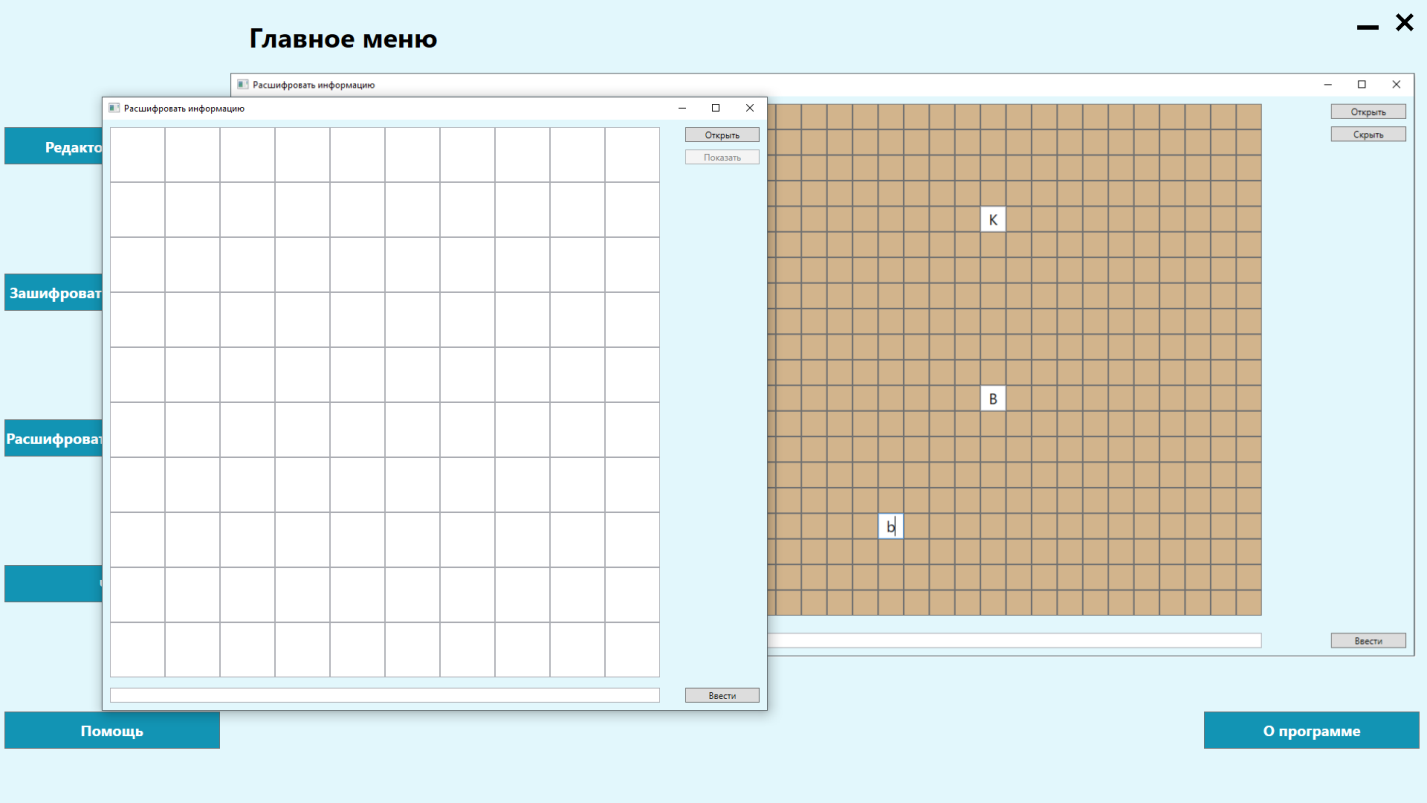


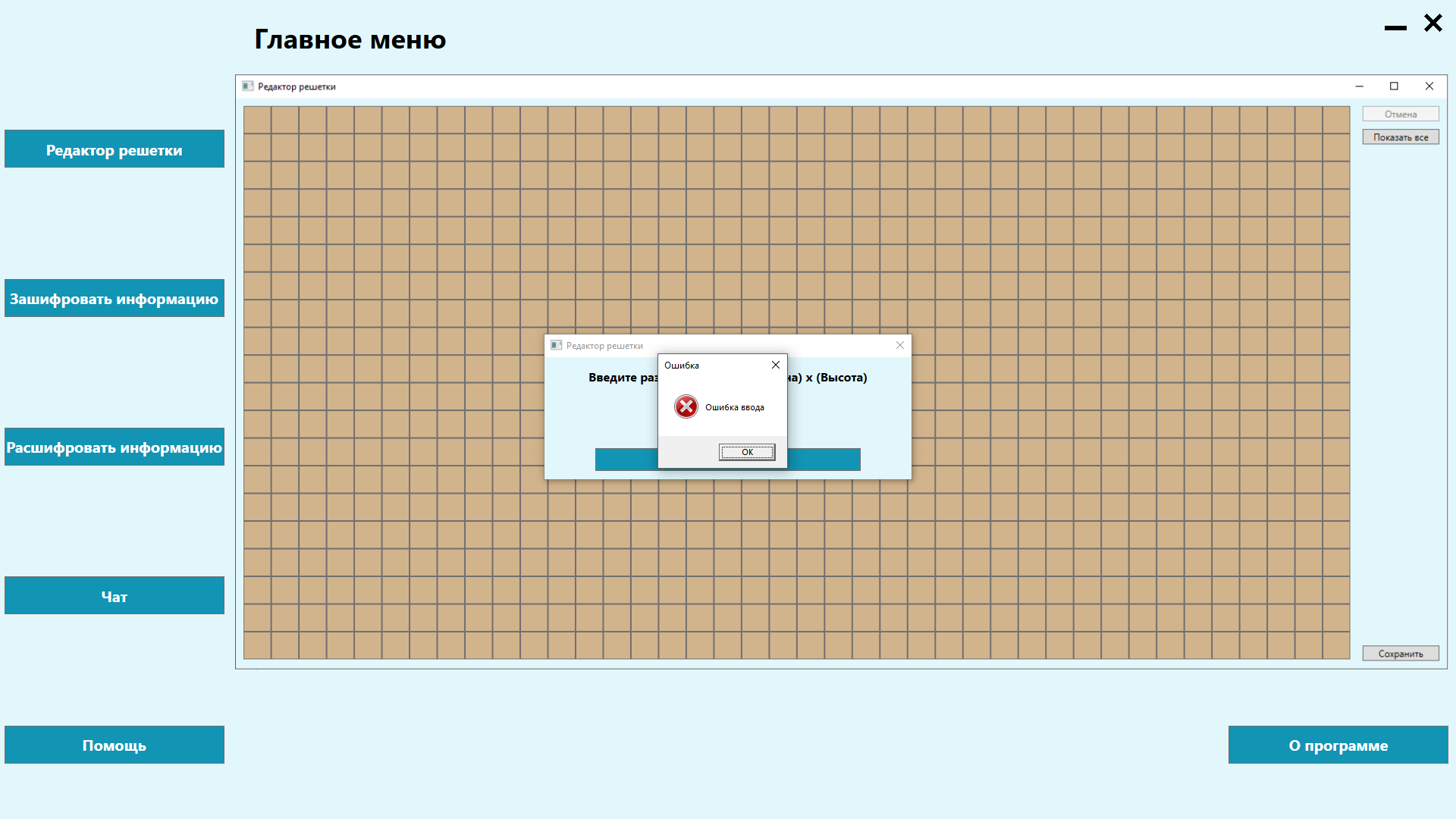
Рисунок 16. InformationDecoder

**Дополнительные функции:**

1. Общение зашифрованными данными через Интернет-соединение

В главном меню есть кнопка «Чат», которая запускает выбор между сервером и клиентом

Для запуска необходимо ввести ip и порт. Если ввести неверные данные, то программы выдаст сообщение:



Если ip адрес сервера окажется неприемлемым для данного компьютера или сервер, к которому подключаются, не существует, то появится соответствующее сообщение с ошибкой.

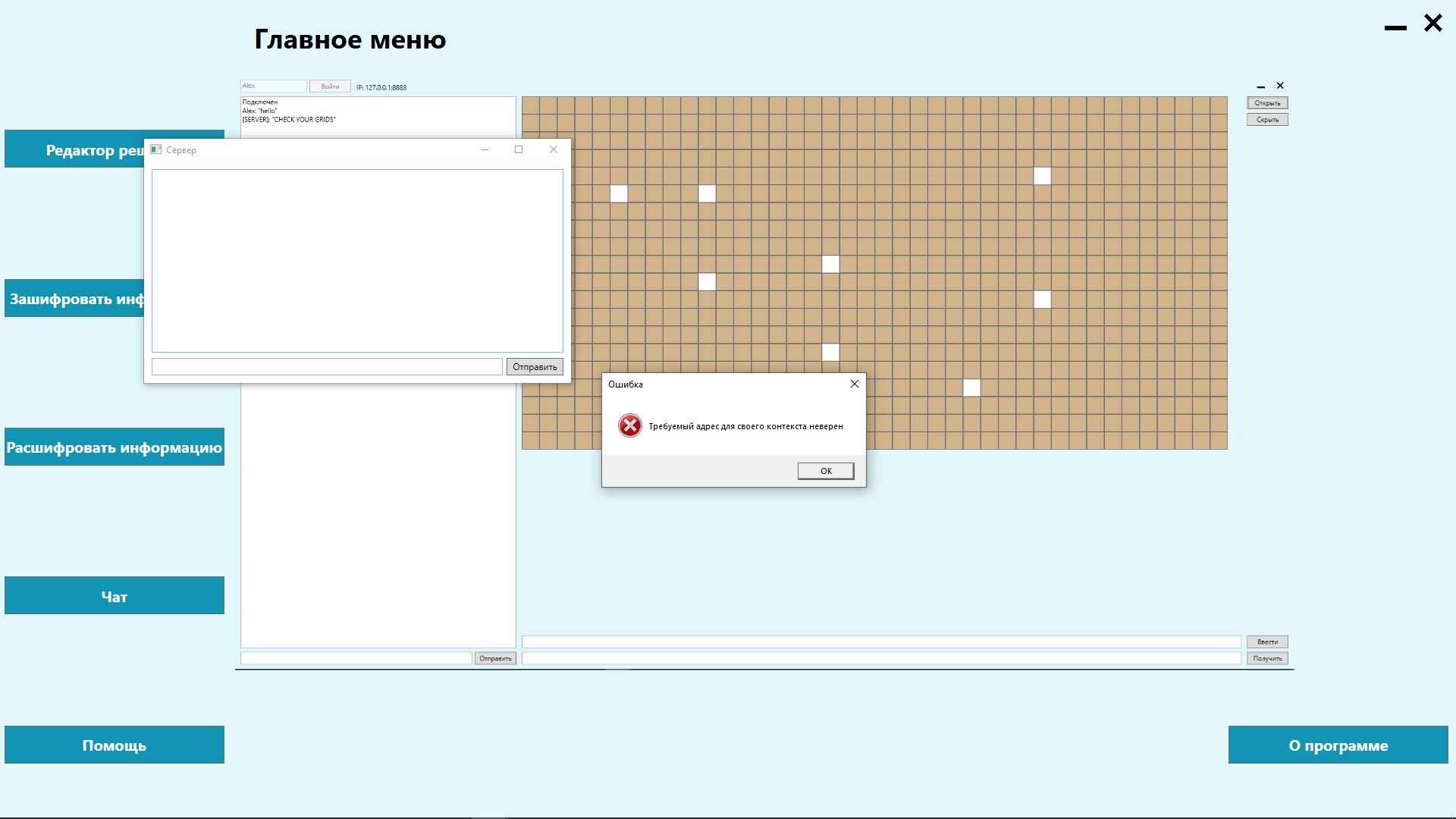
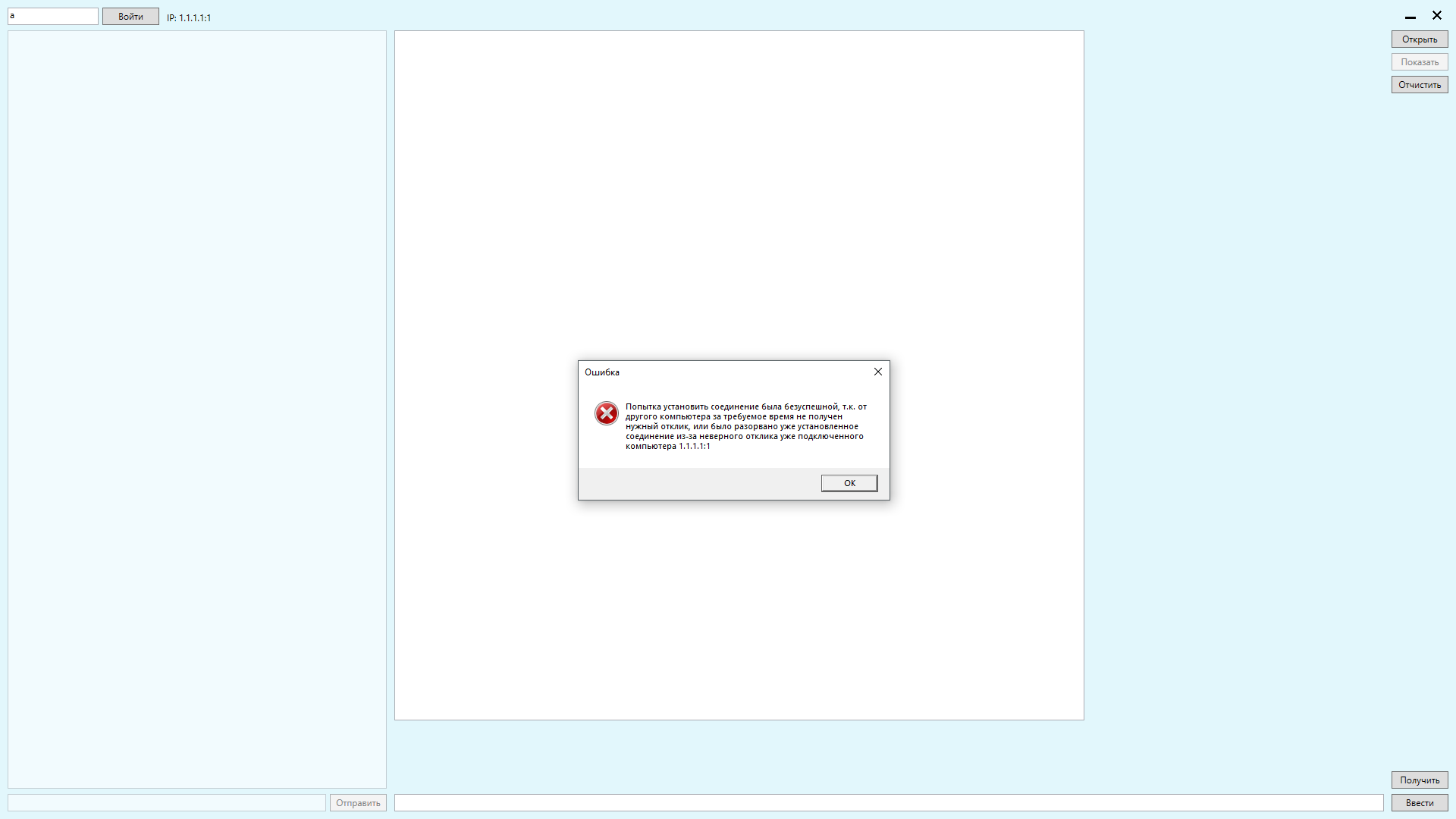


Рисунок 18. Client

Рисунок 17. Server

1. Теоретическая справка.

В главном меню есть кнопка «О программе», которая запускает теоретическую справку (рис. 19)

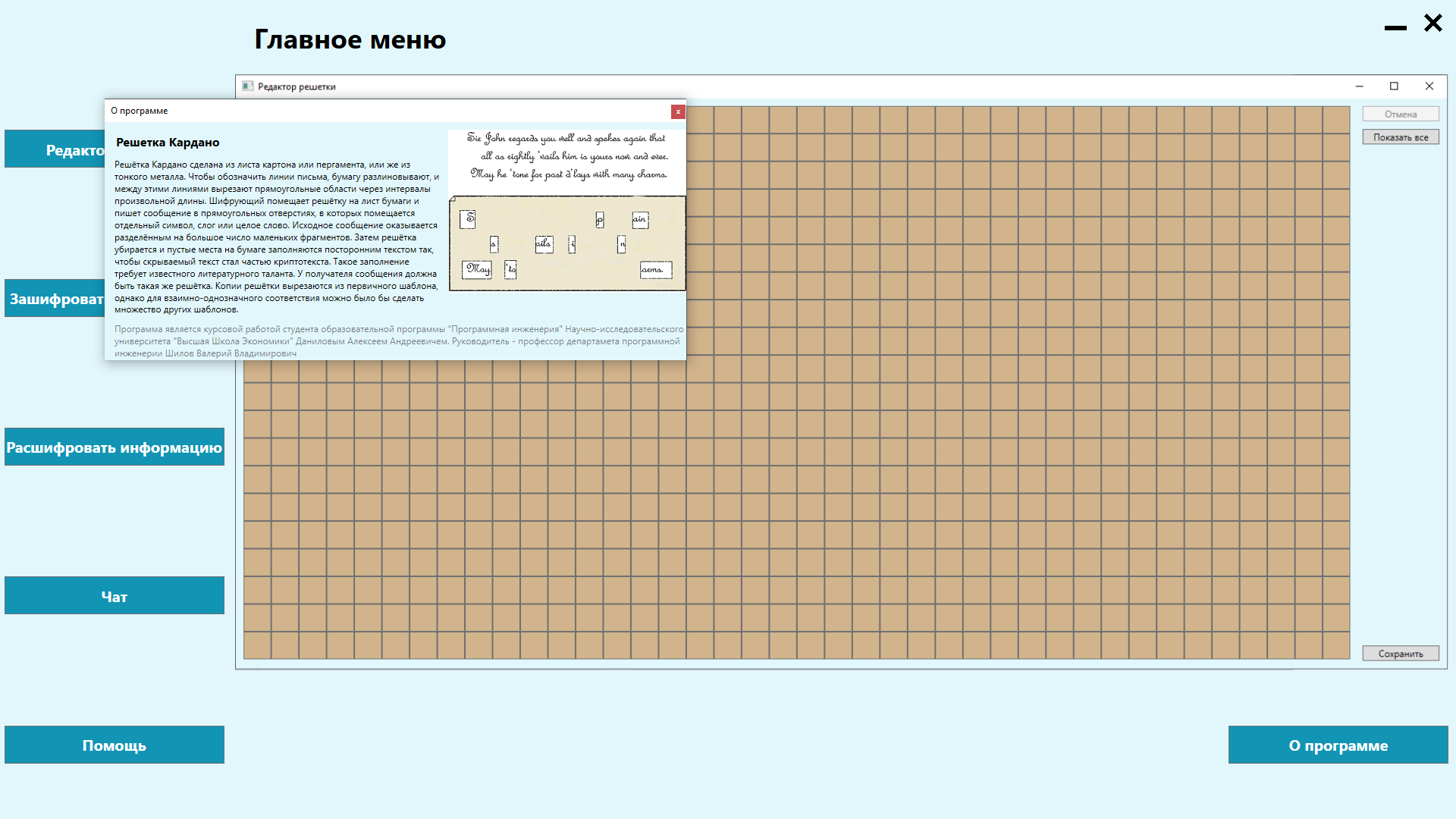


Рисунок 19. AboutProgramm

# ПРИЛОЖЕНИЕ 1

**ТЕРМИНОЛОГИЯ**

Таблица

|  |  |
| --- | --- |
| **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.

**ПРИЛОЖЕНИЕ 3**

**СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ**

1. ГОСТ 19.101-77 Виды программ и программных документов. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
2. ГОСТ 19.102-77 Стадии разработки. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
3. ГОСТ 19.103-77 Обозначения программ и программных документов. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
4. ГОСТ 19.104-78 Основные надписи. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
5. ГОСТ 19.105-78 Общие требования к программным документам. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
6. ГОСТ 19.106-78 Требования к программным документам, выполненным печатным способом. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
7. ГОСТ 19.201-78 Техническое задание. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
8. ГОСТ 19.603-78 Общие правила внесения изменений. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
9. ГОСТ 19.604-78 Правила внесения изменений в программные документы, выполненные печатным способом. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
10. ГОСТ 15150-69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды. – М.: Изд-во стандартов, 1997.
11. ГОСТ 19.301-79 Программа и методика испытаний. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
12. В. В. Ященко // Введение в криптографию. - М.: МЦНМО, 2000. — 271 с.

# **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 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |