**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение

высшего образования

**«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра «Измерительно-вычислительные комплексы»

Приложение «Го-Бан»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Листов 8

**Руководитель разработки**:

профессор каф. ИВК, к.т.н., доцент

*Шишкин Вадим Викторинович*

« » 2022 г.

**Исполнитель**:

студент гр. ИСТбд-22

*Бартецкий Павел Витальевич*

« »

2022г.

**2022**

**Введение**

Наименование игры: Го-бан

Наименование разрабатываемой игры: Go-ban the game

Выбранная структура данных для эмуляции игровой доски в гобан, это двумерный список. Строка такой матрицы отвечает за координату x а столбец за координату y.

Для хранения данных пользователей, выбран список словарей. Словарь следующего вида:

* name: имя пользователя
* color: цвет камней, которыми играет пользователь
* lose: количество проигрышей пользователя
* win: количество побед пользователя

Для сохранения массива словарей используется файл с расширение json, так как python словарь и json схожи по формату. Файл перед сохранением шифруется.

**1. Технические характеристики**

**1.1 Постановка задачи на разработку приложения**

Определяется общей постановкой задачи в задании на курсовую работу

**1.2 Математические методы**

Математические методы не используются.

**1.3 Алгоритмы**

1.3.1 Алгоритм хода компьютера

Воспользуемся алгоритмом minimax. Этот алгоритм минимизирует возможные потери, которые лицо, принимающее решение не может предотвратить при развитии событий по наихудшему для него сценарию.

Для начала нужно описать основные паттерны в Го-бан.

* Пять подряд, это победный паттерн
* Открытая четверка, это паттерн тоже является победным, так как противник не сможет закрыть 4 ваших фишки с двух сторон
* Закрытая четверка, этот паттерн похож на предыдущий, но с одной его стороны, стоит вражеская фишка.

Аналогом этого паттерна является, четыре фишки разделены пустотой

* Открытая тройка, это три фишки в ряд или 3 фишки разделенный одним разрывом.
* Также есть открытые и закрытые двойки.

Описав все это, можно выдать данным паттернам очки, по которым алгоритм будет проверять и выявлять лучший вариант:

Пять в ряд 10 000, открытая четверка 1000, закрытая четверка 500, четверка с брешью 400 и так далее.

Помимо основного алгоритма, есть и другие алгоритмы:

* Получение цвета фишки алгоритм проверяет текущую клетку или клетку со смещение и возвращает чилосове значение, для компьютера это 2, для игрока 1
* Алгоритм получения клетки доски, данный алгоритм необходим чтобы по щелчку определить клетку на доске
* Алгоритм для проверки, можно ли поставить фишку на клетку
* Алгоритм для получения всех 4х направлений от точки на которую сходили. Возвращает количество фишек на линии
* Алгоритм проверки победы, проверяет собрались ли 5 фишек одного цвета подряд в одной линии
* Алгоритм отрисовки графики, сначала рисуем грани доски, потом рисуем линии сетки, а потом рисуем украшения как на оригинальной доске ГО.
* Основной алгоритм, с помощью которого AI выбирает клетку для хода. Происходит подсчет очков, если атакующий ход стоит больше чем защитный, то ai составляет свою последовательность, иначе блокирует последовательность игрока.

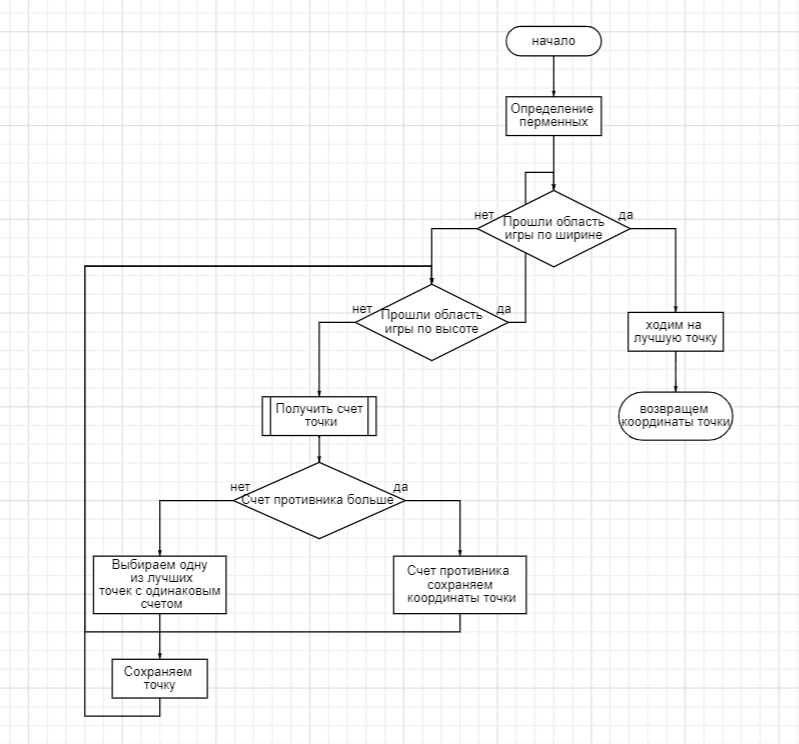


Рисунок 1 - Ход компьютера основываясь на стоимости хода

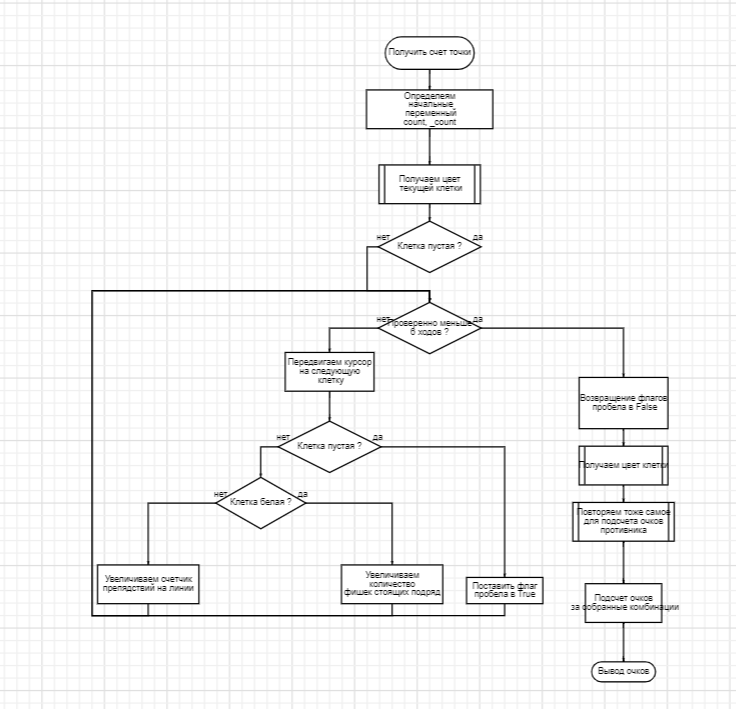


Рисунок 2 - Подсчет очков для хода

1.3.2 Алгоритм шифрования/дешифрования RC5

Для шифрования выбран алгоритм симметричного шифрования RC5.

Процедура шифрования состоит из двух этапов, первый это процедура расширения ключа. А второй это само шифрования.

Для расширения ключа, необходимо выровнять ключ, инициализировать массив расширенных ключей и перемешать массив ключей.

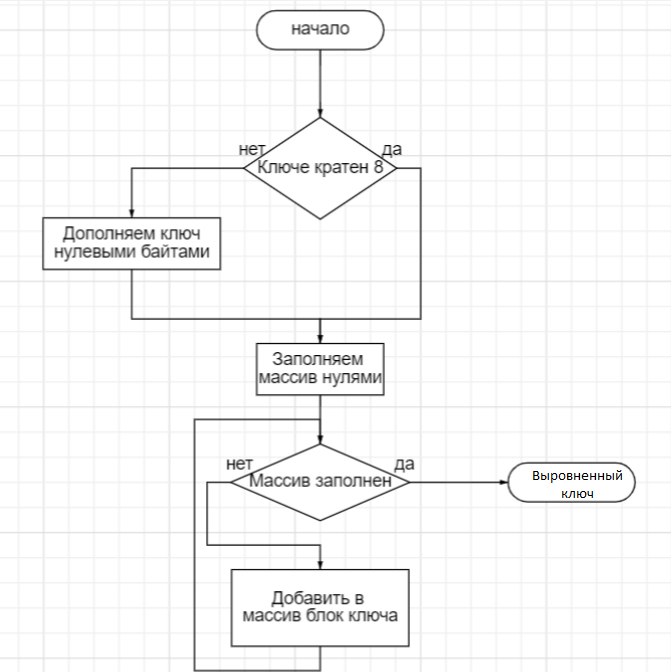


Рисунок 3- Выравнивание ключа

Алгоритм представляет собой сеть Фейсстеля, в каждом раунде происходит следующее, кроме нулевого:



где

r это номер текущего раунда, начиная с 1

S это фрагмент расширенного ключа

<<<n операция циклического сдвига на n битов влево

В нулевом раунде выполняется операции наложения двух первых фрагментов расширенного ключа на шифруемые данные

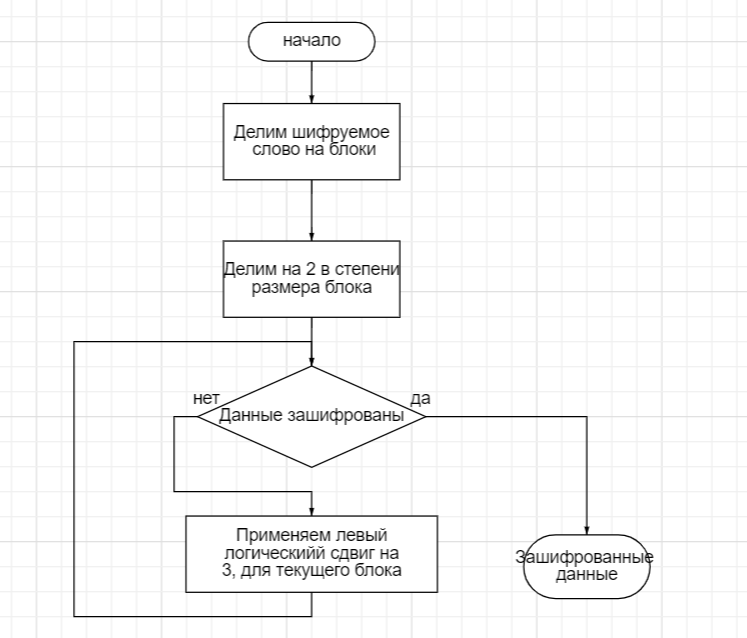


Рисунок 4 - Шифрование данных

Алгоритм дешифрования происходит в обратном порядке шифрования:



>>> n - операция циклического сдвига вправо

r - номер раунда в обратном порядке, т.е. начиная с R и заканчивая единицей.

В конце выполняется обратные операции и для нулевого раунда.

**2. Источники, использованные при разработке**

1. Блок о шифровании. - URL: <http://crypto.pp.ua/2011/01/algoritm-rc5> (дата обращения: 13.12.2020). - Текст: электронный
2. Жданов, Н. А. Алгоритм "минимакс" и его реализация на примере игры "крестики-нолики" / Н. А. Жданов, Ю. М. Бурханова, Ю. О. Воронецкий // Политехнический молодежный журнал. – 2019. – № 5(34). – С. 4. – DOI 10.18698/2541-8009-2019-5-482. – EDN WDYDNX.
3. Прокин, А. А. Методы защиты и шифрования информации / А. А. Прокин, К. Д. Радаев // Материалы XXIII научно-практической конференции молодых ученых, аспирантов и студентов Национального исследовательского Мордовского государственного университета им. Н. П. Огарёва : в 3 частях, Саранск, 21–28 мая 2019 года. – Саранск: Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва, 2019. – С. 271-275. – EDN HEASIA.
4. Алгоритмы для оценки ходов в играх антагонистического типа / Е. С. Белашова, Р. Р. Хабибулин, Б. Р. Шарипов, К. Ю. Канбекова // Вестник Технологического университета. – 2019. – Т. 22. – № 8. – С. 130-134. – EDN IRAZFN.