Построение биодатчика случайных чисел

и оптимизация его характеристик с помощью вычислительных экспериментов

Задорожный Д.И., Коренева А.М., Фомичёв В.М.

Код безопасности

конференция РусКрипто

Введение

- Биологический датчик случайных чисел (БиоДСЧ) разработан с целью генерации пользователем массива случайных бит. Оценочная производительность не менее 10 бит/сек.
- В докладе рассматривается макет БиоДСЧ, основанного на скорости и точности реагирования руки пользователя на изменение изображения на экране персонального или планшетного компьютера.
- Описано устройство одного класса БиоДСЧ и вычислительные эксперименты по оптимизации характеристик датчика.

Код Безопасности

Требования к БиоДСЧ

Для генерации СП пользователи могут использовать БиоДСЧ на основе персонального или планшетного компьютера

Особенности среды функционирования определяют общие требования к БиоДСЧ:

1. Удобство для пользователя работы с БиоДСЧ
2. 1 сессия работы с БиоДСЧ реализуется не более чем за 30 секунд
3. Генерация за 1-2 сессии 320 бит (что соответствует в алгоритме ГОСТ 28147-89 сумме длин ключа и вектора инициализации – 256+64 бит)

Задача пользователя

Задача пользователя – сгенерировать *M* случайных бит.

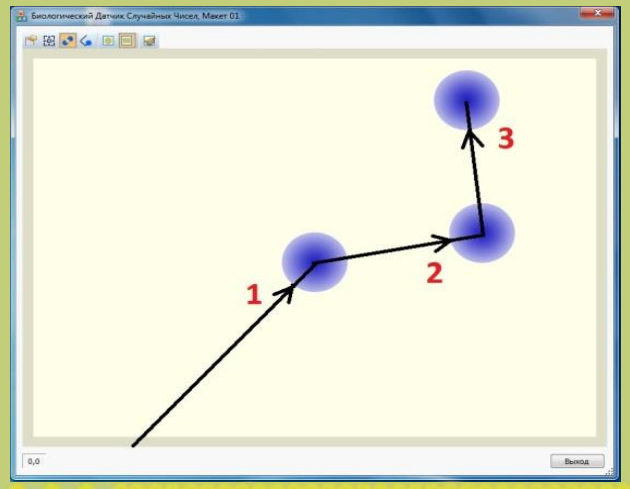
Генерируемые случайные последовательности (СП) получаются с помощью **осмысленных реакций пользователя в случайные моменты времени** на некоторый достаточно сложно устроенный псевдослучайный процесс с рядом меняющихся во времени характеристик.

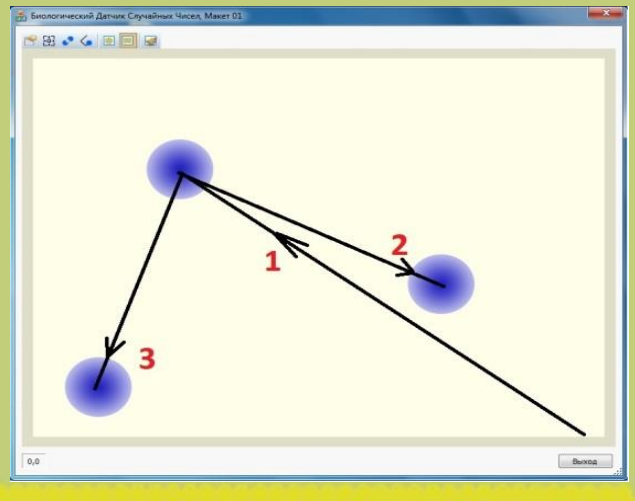
Меняющиеся характеристики процесса подвергаются измерению в случайные моменты времени, определяемые моторикой руки пользователя, и отображаются в случайный массив бит.

Код Безопасности

Описание псевдослучайного процесса

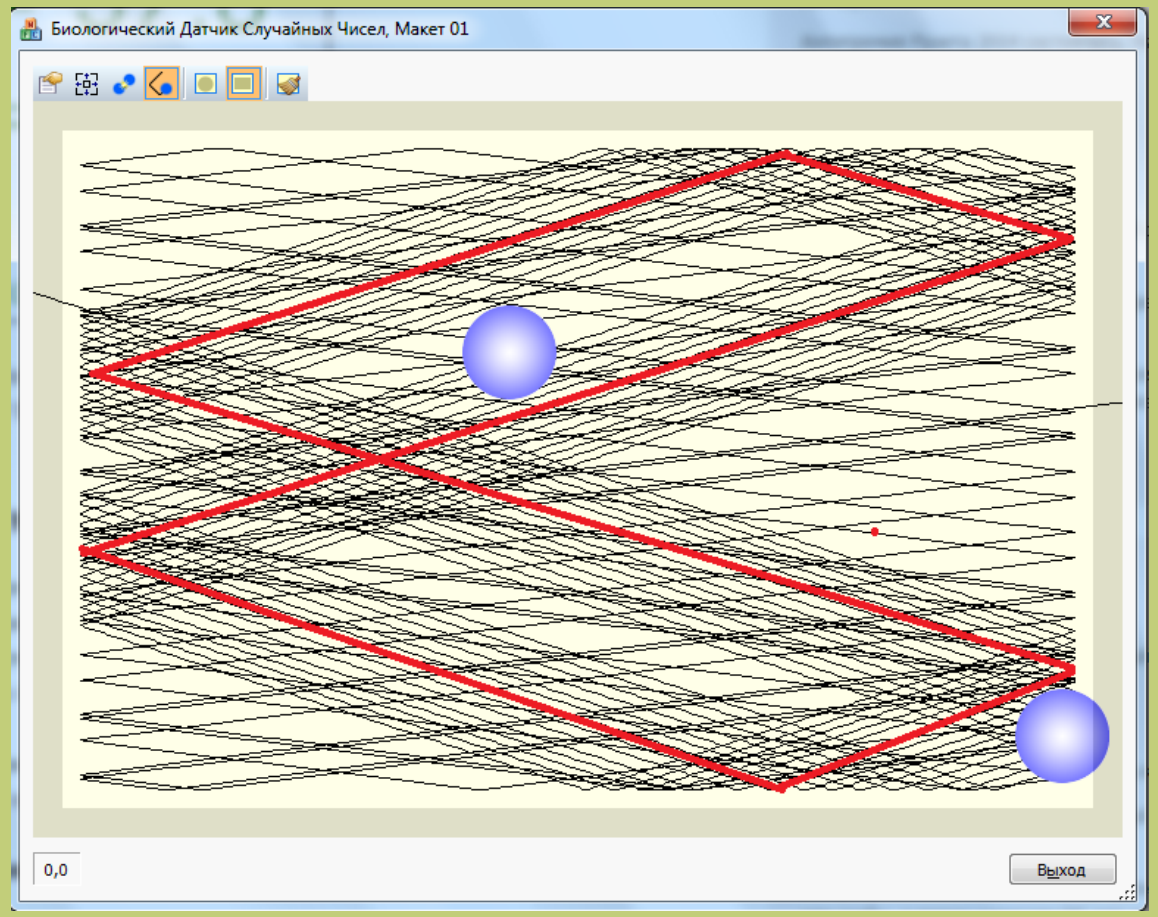
На мониторе персонального или планшетного компьютера последовательно генерируются через доли секунды N прямолинейно движущихся кругов диаметра d; i-й круг генерируется из центра прямоугольной рабочей области (ПРО) в момент i-го клика пользователя (в случае планшета – нажатия пальцем), $i=1,\ldots,N$; круги стартуют в моменты кликов с заданной скоростью v из центра ПРО в направлениях $W_1,\ldots,W_N$, задаваемых невидимым для пользователя «вектором вылета кругов» с началом в центре ПРО, вращающимся с заданной угловой скоростью Ω. Допустимы различные варианты генерации кругов в момент i-го клика пользователя:

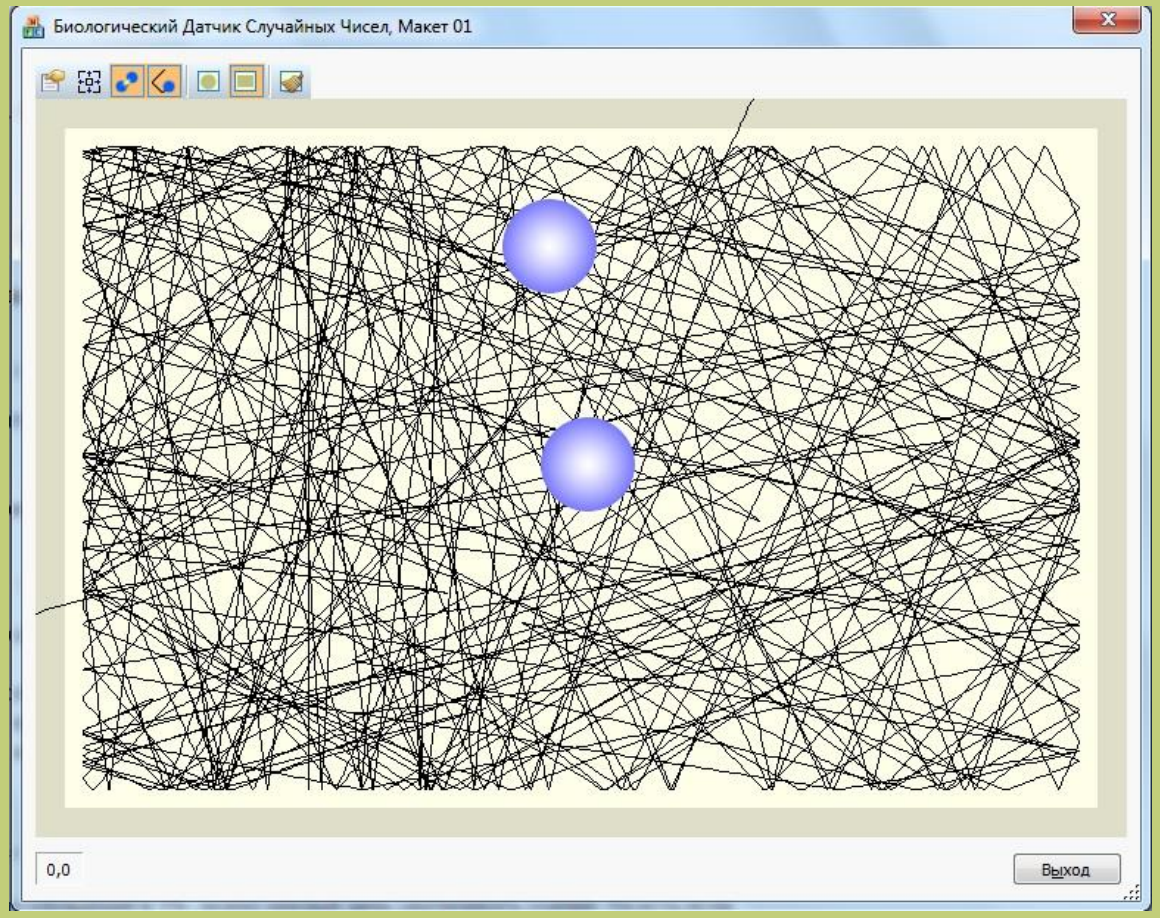




Круги движутся подобно проекциям шаров на бильярдном столе, отражаясь друг от друга и от границ ПРО.

Описание псевдослучайного процесса





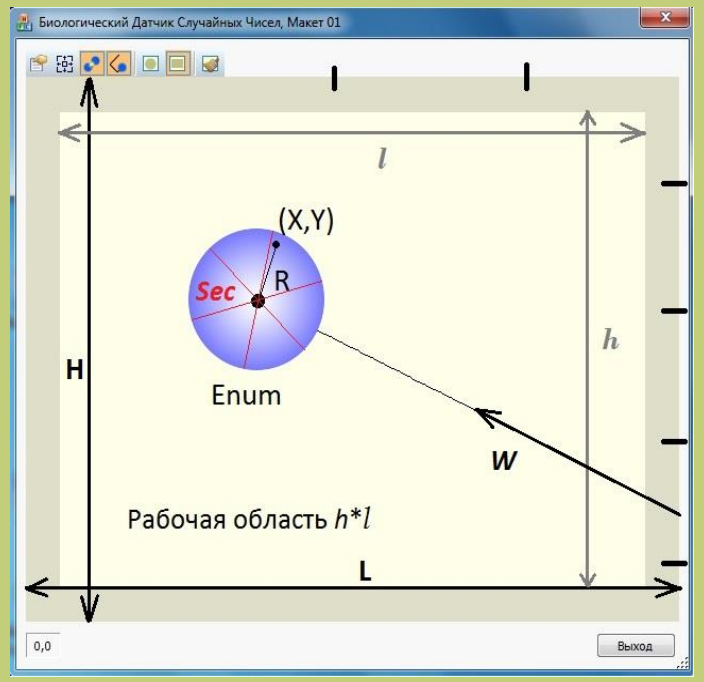
Круги движутся подобно проекциям шаров на бильярдном столе, отражаясь друг от друга и от границ ПРО.

Код Безопасности

Описание действий пользователя

Действия пользователя:

после появления в ПРО всех N кругов последовательно удалить эти круги, быстро кликая в площадь каждого круга мышью (в случае планшета пальцем).

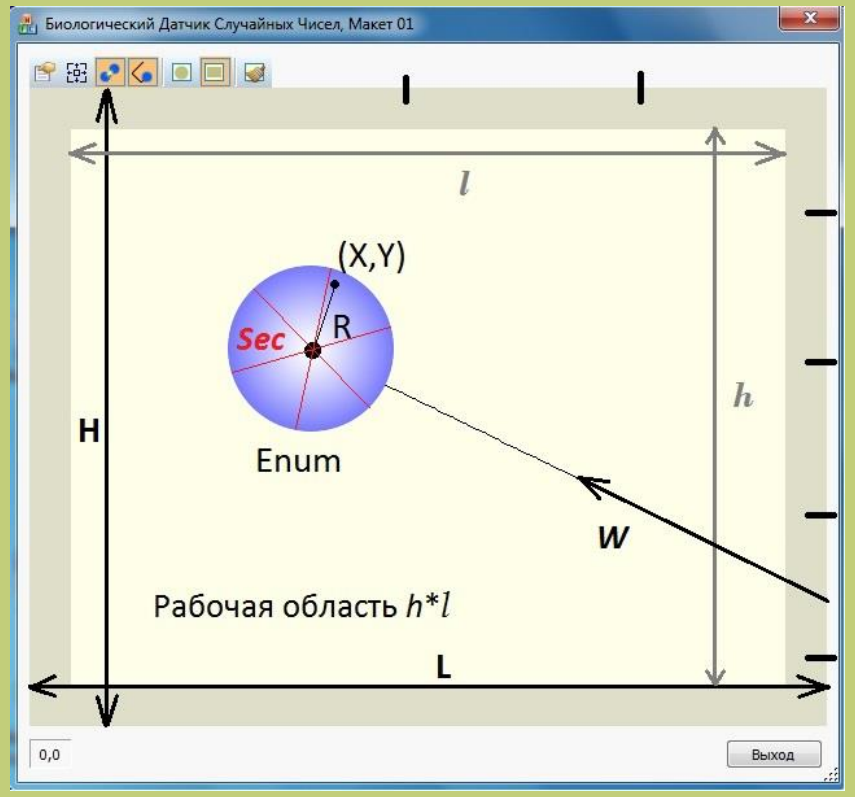


Каждый круг разделен на 2^k равных невидимых пользователю секторов с номерами от 0 до 2^k-1 и вращается вокруг своего геометрического центра с угловой скоростью ω.

Сеанс генерации некоторого количества битов СП завершается после удаления всех кругов. Если полученное количество битов меньше *M*, то сеанс повторяется столько раз, сколько необходимо для получения *M* битов.

Код Безопасности

Определение массива двоичных чисел



В момент попадания (успешного клика) по *i*-му кругу измеряются следующие характеристики процесса («источники энтропии»), $i=1,\ldots,N$:

- координата X_i внутри ПРО точки попадания по *i*-му кругу;
- координата Y_i внутри ПРО точки попадания по *i*-му кругу;
- расстояние R_i от центра *i*-го круга до точки попадания внутри круга;
- номер сектора Sec_i попадания внутри *i*-го круга на расстоянии от центра, превышающем 3 пикселя;
- номер круга $Enum = i$;
- время t_i реагирования пользователя на *i*-й круг, $i>1$, вычисляемое как разность между моментами попадания в *i*-й круг и в $(i-1)$-й круг, вычисляемых с помощью счетчика тактов процессора, обеспечивающего высокую точность.

Измеренные характеристики переводятся в двоичное представление, элементы которого затем фильтруются при включении в результирующий массив битов.

Выбор характеристик предполагает непредсказуемость каждого бита по известным значениям других битов.

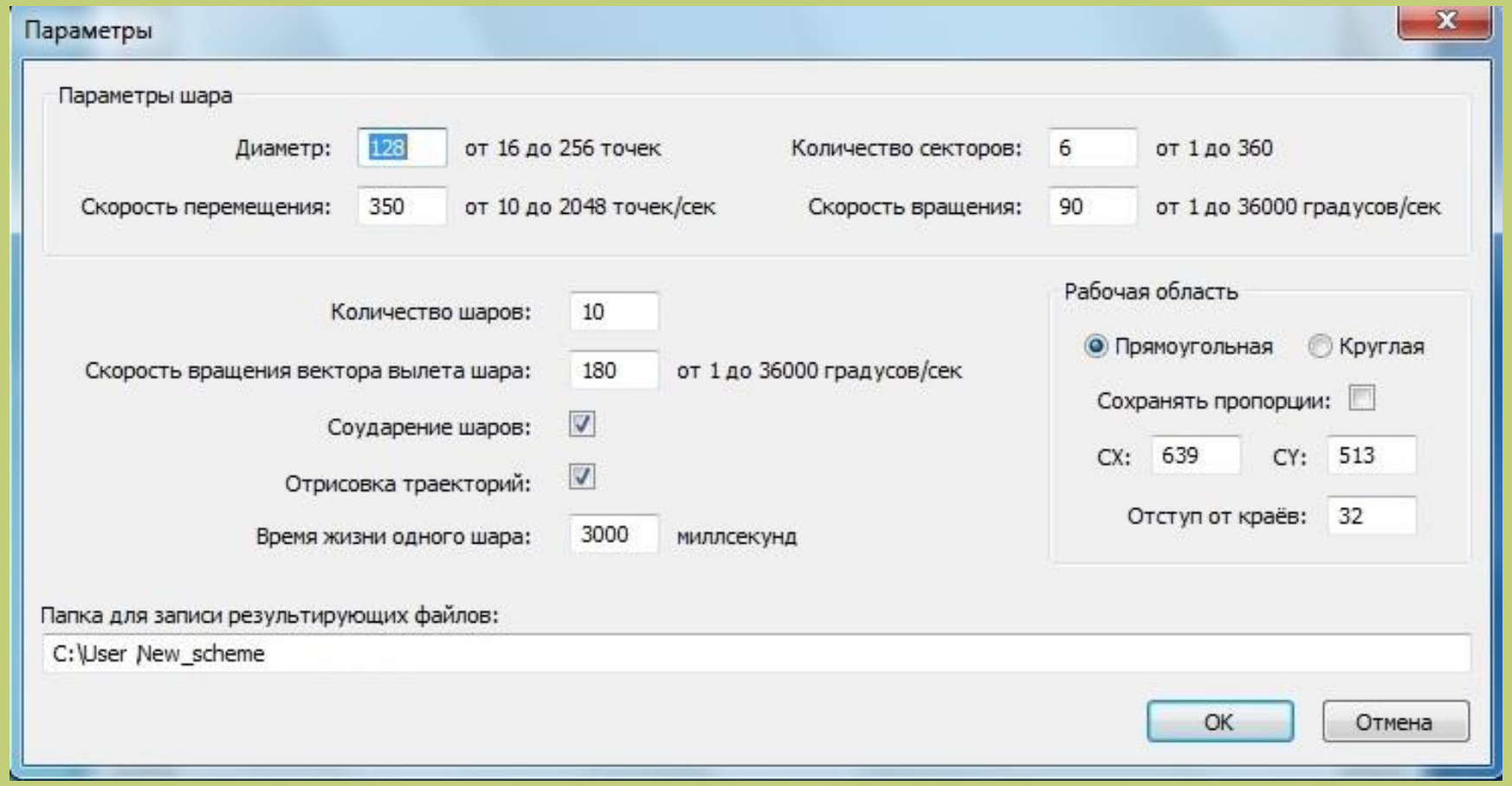
Допущения при анализе данных

- регистрируемые события независимы во времени (реакцию на события, наблюдаемые на мониторе, человеку сложно тиражировать с высокой точностью);
- указанные «источники энтропии» независимы (невозможность вычисления значения одной характеристики по известным значениям других характеристик);
- вычисление доверительных интервалов для значений контролируемых характеристик выполнялось с выбранным уровнем значимости 0.05;
- для распознавания равномерности распределения знаков полученной выборки (после приведения по модулю) применялся критерий хи-квадрат согласия с равномерным распределением.

Количество битов, получаемых со значений каждого источника случайности, определялось эмпирическим путем на основе анализа информационной энтропии значений рассматриваемых характеристик.

Экспериментальные исследования

Возможность установки различных значений параметров макета:



Экспериментальные исследования

Экспериментально определены следующие значения параметров приоритетной реализации БиоДСЧ:

Параметр	Значение	Параметр	Значение
диаметр круга	90 пикселей	**число секторов**	8
количество кругов	10	**рабочая область**	прямоугольная 800×600, отступ от краев 20
скорость перемещения круга	250 пикс./сек	**скорость вращения «вектора вылета кругов»**	3600 град/сек
скорость вращения секторов	7200 град/сек	**время генерации массива**	30000 мс

Выводы

- ✓ Эмпирически установлено, что «уничтожение» каждого круга позволяет получить 30 бит в массиве случайных данных.
- ✓ 1 сессия работы макета БиоДСЧ продолжительностью ≤ 30 секунд позволяет сгенерировать около 300 бит.
- ✓ На практике получено ограничение полюсности p выходной двоичной последовательности: $p \leq 1/2 + -\delta$, где $0 \leq \delta \leq 10^{-2}$
- ✓ Для генерации ключа и вектора инициализации алгоритма ГОСТ 28147-89 достаточно 2 сеансов работы БиоДСЧ.
- ✓ Полученная реализация БиоДСЧ указанным требованиям удовлетворяет.

Для получения необходимых 320 бит в ходе 1 сессии БиоДСЧ перспективным для ПК является увеличение количества кругов на 20-30%.

Представляет интерес как оптимизация параметров разработанного макета, так и исследование других макетов.

Спасибо за внимание!

Ваши вопросы?

Код безопасности