

- оценить альтернативные варианты планировки производства;
- исследовать узкие места в перемещении материальных потоков;
- оценить влияние поведения операторов на показатели производства;
- определить поведение системы в случае поломок оборудования;
- определить вероятность производства бракованной продукции;
- определить, как изменятся показатели производства из-за плановых остановок.

Используя возможности среды AnyLogic можно дополнительно создать библиотеку, которая позволяет включать элементы для быстрого моделирования подобных систем и объектов, систем движения материальных потоков, работу персонала и систем контроля качества продукции.

После построения модели выполняется фаза проекта, связанная с проведением экспериментов, и процесс тестирования множества параметров для поиска оптимального решения. Далее, используя результаты проведенных экспериментов, определялись лучшие типы устройств производственной линии в целом и их конфигурации с точки зрения пропускной способности, количества брака и надежности. Таким образом, получены решения, которые позволили значительно улучшить устройство производственной линии и при минимальных затратах выбрать ее наилучшую конфигурацию.

УДК 004.056:061.68

### ФОРМИРОВАНИЕ СКРЕМБЛИРОВАННОГО ЧАСТОТНО-МОДУЛИРОВАННОГО СИГНАЛА ДЛЯ МАСКИРОВАНИЯ ПЕРЕДАЧИ ИНФОРМАЦИИ

Бокуть Л.В.<sup>1</sup>, Деев Н.А.<sup>2</sup>

<sup>1</sup>Белорусский национальный технический университет, Минск, Республика Беларусь

<sup>2</sup>Объединенный институт проблем информатики НАН Беларуси, Минск, Республика Беларусь

Аналоговое скремблирование относится к классу известных методов маскирования связи и применяется практически во всех современных средствах передачи информации. Суть его состоит в преобразовании исходного речевого сигнала с целью минимизации признаков речевого сообщения, в результате которого этот сигнал становится неразборчивым и неузнаваемым. Необходимым условием такого преобразования является возможность обратного преобразования для восстановления речевого сигнала на приемной стороне [1].

Технические средства, разработанные на основе аналоговых методов скремблирования, часто используются для защиты речевой информации от прослушивания. При аналоговом скремблировании речевого сигнала можно преобразовывать по амплитуде, частоте и времени. Амплитудные преобразования при

Результатом имитационного моделирования и проведения экспериментов с применением полученной модели является повышение эффективности использования оборудования, оптимизация производства, сокращение времени производственного цикла, увеличение объемов производства и улучшение качества готового изделия. Это соответствует всем поставленным в данной работе задачам.

#### Литература

1. Нестеренко А.О., Вислоух С.П. Оптимізація процесів приладобудівного виробництва шляхом імітаційного моделювання [Текст] / Комплексне забезпечення якості технологічних процесів та систем: матеріали тез доповідей VII міжнародної науково-практичної конференції (м. Чернігів, 24–27 квіт. 2017 р.): у 2-х т. / Чернігівський національний технологічний університет [та ін.]; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів: ЧНТУ, 2017. – Т. 2. – С. 143.
2. Маликов, Р.Ф. Практикум по имитационному моделюванню складних систем в середі AnyLogic 6 [Текст]: учеб. пособие / Р. Ф. Маликов. – Уфа: Изд-во БГПУ, 2013. – 296с.
3. Боев В.Д., Кирик Д.И., Сыпченко Р.П. Компьютерное моделирование: Пособие для курсового и дипломного проектирования. — СПб.: ВАС, 2011. — 348 с.

скремблировании не применяются из-за проблем точного восстановления амплитуды речевого сигнала при его обработке.

При частотном преобразовании сигнала используются частотная инверсия сигнала, разбиение полосы частот речевого сигнала на несколько сегментов и частотная инверсия спектра в каждом сегменте относительно его средней частоты, разбиение частоты речевого сигнала на несколько сегментов и их частотные перестановки.

При временных преобразованиях производится разбиение сигнала на речевые сегменты и их перестановка во времени: инверсия по времени сегментов речи, временные перестановки сегментов речевого сигнала. При комбинированных методах преобразования сигнала используют одновременно несколько различных способов скремблирования (как частотных, так и временных), число которых

ограничивается, как правило, возможностями технической реализации аналоговых скремблеров.

Различие скремблеров состоит в числе частот инверсии, скорости их изменения и количестве ключей, определяющих длительность перебора возможных комбинаций изменяемых параметров без их повторения. Некоторое представление об уровне защиты информации может дать показатель количества ключевых параметров. Для частотного инвертора ключевым параметром является значение частоты инверсии сигнала. Размерность этого параметра, то есть число возможных значений частот инверсии (число ключей) с ощутимыми искажениями, возникающими при прослушивании на соседней частоте, не превышает 20–30.

При аналоговом скремблировании преобразованный речевой сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает такую же полосу частот спектра, как и исходный сигнал. Присутствие при передаче в канале связи фрагментов исходного речевого сообщения, преобразованного в частотной и (или) временной областях, означает, что возможен перехват и анализ передаваемой информации на уровне звуковых сигналов. Перехват сообщений возможен при применении специальных средств, позволяющих сначала определить ключевую последовательность (т. е. правила изменения параметров преобразования сигнала), а затем подстроиться под найденную ключевую последовательность [2].

Несмотря на высокое качество и разборчивость восстанавливаемой речи, аналоговые скремблеры обеспечивают в основном лишь низкий или средний, по сравнению с цифровыми системами, уровень защиты информации, однако их практическая реализация проще и дешевле.

При цифровом скремблировании предполагается дискретизация исходного аналогового сигнала и передача его основных компонент путем преобразования их в цифровой поток данных. Этот поток смешивается с некоторой псевдослучайной последовательностью, вырабатываемой ключевым генератором по одному из криптографических алгоритмов. Полученное таким образом сообщение с помощью модема передается в канал связи, на приемной стороне производятся обратные преобразования с целью получения открытого речевого сигнала. Реализация цифрового скремблирования на практике оказывается довольно сложной и дорогостоящей.

Предлагается метод маскирования информации, основанный на формировании и обработке скремблированного частотно-модулированного сигнала, произведением двоичных последовательностей, одна из которых псевдослучайная с известным законом формирования, другая – случайная, формируемая с

помощью источника физического шума и компаратора.

В качестве аппаратных реализаций скремблирования часто используют генератор случайных чисел на сдвиговом регистре с линейной обратной связью. Такая технология маскирования информации является достаточно эффективной. Показателем эффективности здесь служит количество операций, затрачиваемых на вычисление очередного элемента псевдослучайной последовательности. Однако, остается вероятность несанкционированного доступа к информации при применении специальных средств определения ключевой последовательности и подстройки под найденную ключевую последовательность.

Предлагаемое формирование скремблированного частотно-модулированного сигнала, содержащего речевое сообщение произведением двоичных последовательностей, обеспечивает высокую энергетическую скрытность. Во-первых, сформированный частотно-модулированный сигнал не имеет пороговых ограничений по помехоустойчивости и позволяет работать «под шумами», а во-вторых, спектр сигнала в канале не имеет характерных ярко выраженных участков. Добавление случайной компоненты позволяет избежать регулярности спектральных составляющих и тем самым увеличивает число ключевых комбинаций до бесконечности.

На передающей стороне сигнал формируется в соответствии со схемой, приведенной на рисунке 1.

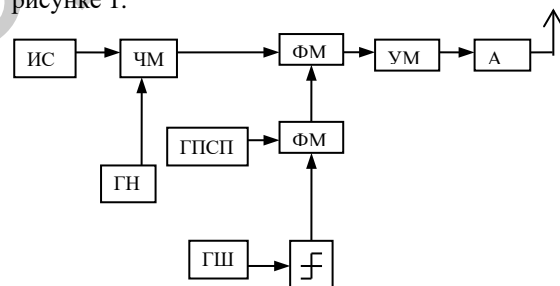


Рисунок 1 – Структурная схема формирования скремблированного сигнала

Источником речевого сообщения (ИС) аналогового сигнала  $\lambda(t)$  формирует низкочастотный сигнал. Генератор несущей частоты (ГН) обеспечивает формирование высокочастотного узкополосного несущего сигнала. В частотном модуляторе (ЧМ) аналоговый сигнал и несущий перемножаются. Сформированный узкополосный частотно-модулированный сигнал поступает на вход фазового манипулятора (ФМ<sub>н1</sub>) и подвергается фазовой манипуляции двоичной последовательностью, представляющей комбинацию псевдослучайной двоичной последовательности (ПСП)  $g(t - \tau) = \{\pm 1\}$  и случайной двоичной последовательности  $X(t) = \{\pm 1\}$ , где  $\tau$  – случайная задержка.

Псевдослучайная двоичная последовательность  $g(t - \tau)$  вырабатывается в генераторе (ГПСП). Одновременно с псевдослучайной последовательностью, сгенерированной генератором, подаётся на фазовый манипулятор (ФМн<sub>2</sub>) случайная последовательность  $X(t)$ , вырабатываемая в генераторе (ГШ) и преобразованная в компараторе в клипированный шум. На фазовом манипуляторе (ФМн<sub>2</sub>) осуществляется операция перемножения  $g(t - \tau)$  и  $X(t)$  и образуется двоичная скремблирующая последовательность:

$$Y(t - \tau) = g(t - \tau) \cdot X(t), \quad (1)$$

где полоса спектра последовательности  $X(t)$  определяется тактовой частотой  $f_T = 1/\tau_0$ , а также формирующим фильтром, включенным в ГШ и меньше полосы спектра ПСП,  $\tau_0$  – длительность элемента ПСП.

Сформированный скремблированный частотно-модулированный сигнал, полученный в результате перемножения в (ФМн<sub>1</sub>), усиливается в усилителе мощности (УМ), подаётся в на модуль

антенно-фидерного устройства (АФУ) и далее в эфир.

Скремблированный частотно-модулированный сигнал можно представить:

$$S(t) = a_0 Y(t - \tau) \cdot \cos[(\omega_0 t + \Psi(t) + \beta)], \quad (2)$$

где  $a_0$  и  $\omega_0$  – известные амплитуда и частота сигнала;

$Y(t) = g(t - \tau) \cdot X(t) = \{\pm 1\}$  – скремблирующая последовательность;

$\beta$  – случайная начальная фаза, равномерно распределенная в интервале  $[0, 2\pi]$ ;

$\Psi(t)$  – частота сигнала, медленно изменяющаяся в соответствии с передаваемым сообщением  $\lambda(t)$ , где  $\lambda(t) = d\Psi(t)/dt$ .

Литература

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – М.: Юниор, 2010. – 501 с.
2. Чердынцев В.А., Деев Н.А. Подавление комплекса помех в каналах связи / В.А. Чердынцев, Н.А. Деев // Известия Белорусской инженерной академии. – 2002. – № 2. – С. 31–36.

УДК 380.001+530.182

## ОЦЕНКА ЭНЕРГИИ СОЛИТОНА ВБЛИЗИ ПОВЕРХНОСТИ МЕТАЛЛА

Князев М.А., Русакевич Д.А.

Белорусский национальный технический университет, Минск, Республика Беларусь

Проблема изучения квантовых солитонных состояний, соответствующих одиночным электронам, является весьма перспективной с точки зрения задач нанoeлектроники [1]. Такие состояния могут быть описаны при помощи решений уравнения Шредингера, учитывающего нелинейное взаимодействие электрона, находящегося у поверхности металла, с мнимыми зарядами, расположенными внутри металла. Модели с мнимыми зарядами широко применяются при изучении квантовых точек. В настоящей работе с использованием подхода, развитого в работе [2], получено приближенное выражение для энергии рассматриваемого солитонного состояния.

Известно, что кулоновское отталкивание электронов не позволяет формировать солитонные состояния. Однако для одного электрона такое отталкивание отсутствует, что позволяет построить самосогласованное решение так, чтобы исключить взаимодействие электрона с его собственным полем. Это можно сделать путем введения потенциала мнимого заряда, предполагая, что такой заряд вблизи поверхности металла (электрода) распределяется в соответствии с распределением плотности заряда электрона  $e^2 |\Psi(\vec{r}, t)|^2$ , где  $e$  – заряд электрона. Тогда соответствующее уравнение Шредингера имеет вид

$$i\hbar \frac{\partial \Psi(\vec{r}, t)}{\partial t} = -\frac{\hbar^2}{2m^*} \Delta \Psi(\vec{r}, t) + V_c(\vec{r}, t) \Psi(\vec{r}, t), \quad (1)$$

где потенциальная энергия взаимодействия электрона с мнимыми зарядами (интегрирование ведется по координатам всех мнимых зарядов) определяется соотношением

$$V_c(\vec{r}, t) = -\frac{e^2}{2\kappa} \int \frac{|\Psi(\vec{r}', t)|^2}{|\vec{r} - \vec{r}'|} d\vec{r}', \quad (2)$$

$|\vec{r} - \vec{r}'|$  – расстояние от мнимого заряда до точки наблюдения,  $d$  – расстояние от заряда (действительного или мнимого) до поверхности электрода,  $\kappa$  – диэлектрическая проницаемость,  $m^*$  – эффективная масса электрона,  $a$  – размер солитона.

Построение точного решения уравнения (1) является очень сложной задачей. Однако, можно найти приближенное решение уравнения (1). В этом случае удастся достаточно просто получить приближенную оценку энергии состояния в зависимости от размера солитона, используя соотношение

$$E(a) = \frac{\hbar^2}{2m} \int |\nabla \Psi(\vec{r}, a)|^2 d\vec{r} + \int |\Psi(\vec{r}, a)|^2 V_c(\vec{r}, t) d\vec{r}. \quad (3)$$

С целью упрощения вычислений рассмотрим задачу в случае одной пространственной переменной. Для электронов, локализованных в квантовом проводе, потенциальная энергия взаимодействия  $V_c(x, t)$  приближенно может быть представлена в виде

$$V_c(x, t) \approx -\frac{e^2}{\kappa} |\Psi(x, t)|^2 \ln\left(\frac{a}{d}\right). \quad (4)$$