

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

**Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«САНКТ-ПЕТЕРБУРГСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ  
им. проф. М. А. БОНЧ-БРУЕВИЧА»  
(СПбГУТ)**

---

**С. С. Владимиров**

**ЗАЩИТА ИНФОРМАЦИИ  
В СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ**

**Лабораторный практикум**

**СПб ГУТ)))**

**Санкт-Петербург  
2019**

УДК XXXXX  
ББК XXXXX  
Х ХХ

Рецензент  
профессор кафедры СС и ПД,  
доктор технических наук *О. С. Когновицкий*

*Рекомендован к печати редакционно-издательским советом СПбГУТ*

**Владимиров, С. С.**

Х ХХ      Защита информации в системах передачи данных : лабораторный практикум / С. С. Владимиров ; СПбГУТ. — СПб, 2019. — 20 с.

Учебное пособие призвано ознакомить студентов старших курсов с принципами построения систем передачи данных. Представленный материал служит справочным и методическим пособием при выполнении курса лабораторных работ по дисциплине «Защита информации в системах передачи данных».

**УДК XXXXX  
ББК XXXXX**

© Владимиров С. С., 2019  
© Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», 2019

## Содержание

<b>1. Изучение программы моделирования Logisim.</b>	4
1.1. Цель работы.	4
1.2. Рекомендуемая литература	4
1.3. Теоретическая справка	4
1.4. Порядок выполнения задания	4
1.5. Порядок защиты практической работы.	7
<b>2. Изучение инструмента визуального моделирования Xcos из пакета Scilab</b>	8
2.1. Цель работы.	8
2.2. Рекомендуемая литература	8
2.3. Теоретическая справка	8
2.4. Порядок выполнения задания	8
2.5. Порядок защиты практической работы.	12
<b>3. Практическая работа. Изучение принципа работы цифрового скремблера/дескремблера</b>	13
3.1. Цель работы.	13
3.2. Рекомендуемая литература	13
3.3. Порядок выполнения задания	13
3.4. Порядок защиты практической работы.	15
<b>4. Построение цифрового скремблера/дескремблера в симуляторе Logisim.</b>	16
4.1. Цель работы.	16
4.2. Рекомендуемая литература	16
4.3. Порядок выполнения задания	16
4.4. Порядок защиты практической работы.	17
<b>5. Построение цифрового скремблера/дескремблера в симуляторе Scilab/Xcos</b>	18
5.1. Цель работы.	18
5.2. Рекомендуемая литература	18
5.3. Порядок выполнения задания	18
5.4. Порядок защиты практической работы.	19

# 1. Изучение программы моделирования Logisim

## 1.1. Цель работы

Изучить общие принципы работы с системой моделирования Logisim.

## 1.2. Рекомендуемая литература

1. Logisim: Документация // Официальный сайт Logisim.

URL: <http://www.cburch.com/logisim/ru/docs.html>

## 1.3. Теоретическая справка

Справка написана для версии программы из репозитория ОС Debian Linux, используемой в лабораториях кафедры.

### 1.3.1. Запуск системы Logisim

Программа Logisim запускается через пункт главного меню «Logisim» либо соответствующей командой в терминале.

Команда для вызова Logisim

---

```
user@host: [~]$ logisim
```

---

## 1.4. Порядок выполнения задания

Задание выполняется каждым учащимся индивидуально. Результаты заданий лабораторного практикума и соответствующих заданий практикума должны совпадать.

Отчёт формируется в электронном виде в формате PDF и отправляется на электронную почту преподавателя.

### 1.4.1. Построение простейшей схемы «Логическое И»

Построить простейшую схему, состоящую из двух входов, элемента «Логическое И» (AND) и выхода (рис. 1.1). Научиться смотреть таблицу истинности схемы. При выполнении задания рекомендуется использовать встроенную справку Logisim раздел «Пособие начинающего».

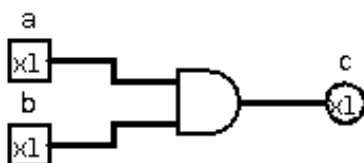


Рис. 1.1. Схема «Логическое И»

1. Разместить на холсте два входных контакта (квадратные), выходной контакт (круглый) и логический элемент AND по образцу рис. 1.1. Эти элементы вынесены на панель инструментов программы. В свойствах контактов задать их имена (метки) по образцу рис. 1.1.

2. Используя инструмент «Рука» из панели инструментов, изменять значения входных контактов и следить, как меняется значение на выходном контакте. Сравнить с таблицей истинности элемента AND.

3. Просмотреть таблицу истинности построенной схемы, используя пункт главного меню «Проект» – «Анализировать схему» – вкладка «Таблица». Сверить с таблицей из пособия.

### 1.4.2. Построение одноразрядного полусумматора

Построить одноразрядный полусумматор на основе базовых логических элементов и на основе элементов XOR (рис. 1.2), используя один набор входов для обеих схем. Научиться использовать тоннели.

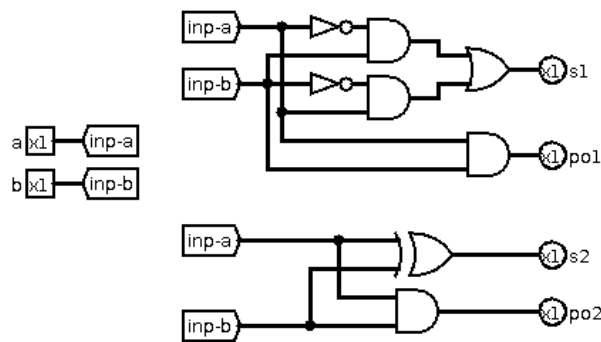


Рис. 1.2. Варианты схемы одноразрядного полусумматора

1. Построить схему по образцу рис. 1.2. В свойствах контактов задать соответствующие метки. Входные контакты подключить к тоннелям («Проводка» — «Тоннель»). Направление и метка тоннеля и задаются в его свойствах.

2. Используя инструмент «Рука» из панели инструментов, изменять значения входных контактов и следить, как меняется значение на выходных контактах. Убедиться, что контакты «s1»/«s2» и «po1»/«po2» показывают равные значения. Сравнить с таблицей истинности одноразрядного полусумматора.

3. Просмотреть таблицу истинности построенной схемы, используя пункт главного меню «Проект» – «Анализировать схему» – вкладка «Таблица». При появлении предупреждения «Выражение неопределено» нажать кнопку «ОК». Сверить с таблицей из пособия.

### 1.4.3. Построение линии задержки и блоков ввода и вывода

Построить линию задержки на одноразрядных регистрах (рис. 1.3). Научиться создавать входной сдвиговый регистр для записи в него начальных значений и выходной сдвиговый регистр для просмотра результата.

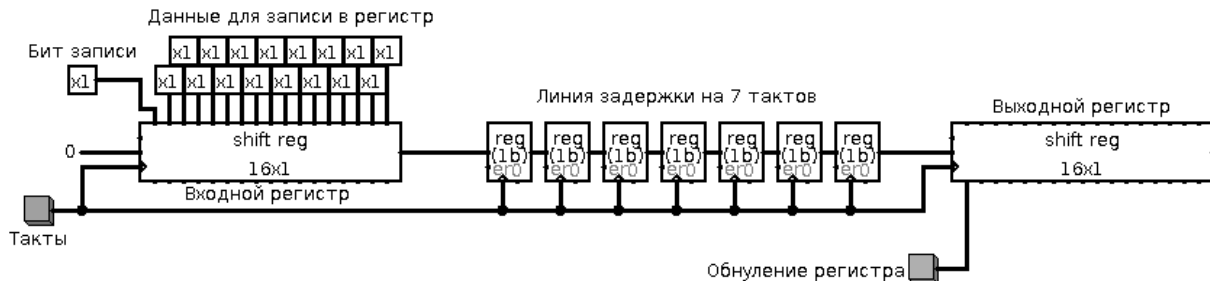


Рис. 1.3. Схема линии задержки на 7 тактов

1. Построить схему по образцу рис. 1.3. Входной и выходной регистры должны иметь разрядность («Биты данных»), равную 1, и длину («Количество ступеней») 16. В свойствах регистров, формирующих линию задержки, указать разрядность («Биты данных»), равную 1. На центральный западный вход входного сдвигового регистра подать однобитовую константу «0». «Бит записи» исходно должен быть равен 0.

2. Используя инструмент «Рука» из панели инструментов, задать начальные данные для записи во входной регистр.

3. Установить «Бит записи» в «1». Затем однократно нажать кнопку «Такты». Убедиться, что входной регистр проинициализировался. Установить «Бит записи» в «0».

4. Последовательным нажатием кнопки «Такты» передавать биты из входного регистра в линию задержки и далее в выходной регистр. Убедиться, что линия действительно вносит задержку в 7 тактов.

5. Обнулить выходной регистр нажатием соответствующей кнопки.

### 1.4.4. Построение линии задержки с внесением помехи

Построить линию задержки с внесением помехи (рис. 1.4).

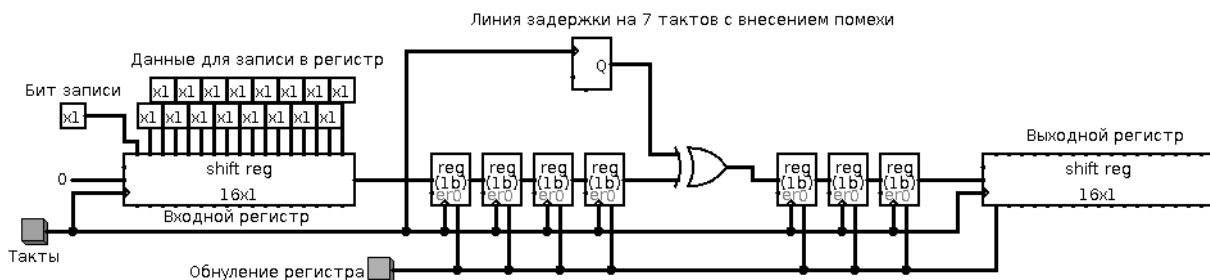


Рис. 1.4. Схема линии задержки на 7 тактов с внесением помехи

1. Построить схему по образцу рис. 1.4. Генератор случайных чисел, играющий роль источника помех, должен иметь разрядность, равную 1. Стоит отметить, что такая схема аналогична двоичному симметричному каналу с вероятностью битовой ошибки 0,5.

2. Используя инструмент «Рука» из панели инструментов, задать начальные данные для записи во входной регистр.

3. Установить «Бит записи» в «1». Затем однократно нажать кнопку «Такты». Убедиться, что входной регистр проинициализировался. Установить «Бит записи» в «0».

4. Последовательным нажатием кнопки «Такты» передавать биты из входного регистра в линию задержки и далее в выходной регистр (всего 23 такта). Сравнить полученный результат с исходными данными.

5. Обнулить выходной регистр и регистры линии задержки нажатием соответствующей кнопки.

### **1.5. Порядок защиты практической работы**

Защита работы может осуществляться одним из нижеперечисленных способов или их сочетанием на усмотрение преподавателя.

1. Устный ответ по теме работы.
2. Тестирование по теме работы
3. Задача по теме работы.
4. Иные варианты на усмотрение преподавателя.

## 2. Изучение инструмента визуального моделирования Xcos из пакета Scilab

### 2.1. Цель работы

Изучить общие принципы работы с инструментами визуального моделирования Xcos из пакета Scilab.

### 2.2. Рекомендуемая литература

1. Справка Scilab // Официальный сайт Scilab.  
URL: [https://help.scilab.org/docs/5.5.1/ru\\_RU/index.html](https://help.scilab.org/docs/5.5.1/ru_RU/index.html)
2. Чингаева, А. М. Визуальное моделирование в Scilab: Xcos. / А. М. Чингаева. — Самара : ПГУТИ. 2012.

### 2.3. Теоретическая справка

Справка написана для версии программы из репозитория ОС Debian Linux, используемой в лабораториях кафедры.

#### 2.3.1. Запуск системы Scilab и инструмента моделирования Xcos

Программа Scilab запускается через пункт главного меню «Scilab» либо соответствующей командой в терминале.

Команда для вызова Logisim

---

```
user@host: [~]$ scilab
```

---

Для запуска инструмента визуального моделирования Xcos необходимо использовать пункт главного меню Scilab «Инструменты»–«Визуальное моделирование Xcos».

### 2.4. Порядок выполнения задания

Задание выполняется каждым учащимся индивидуально. По результатам выполнения работы должен быть написан отчет.

Отчёт формируется в электронном виде в формате PDF и отправляется на электронную почту преподавателя.

#### 2.4.1. Построение одноразрядного полусумматора

Построить одноразрядный полусумматор на основе базовых логических элементов (рис. 2.1). Научиться использовать тоннели.

1. Построить схему по образцу рис. 2.1.
  - Добавить на рабочее поле блок завершения симуляции ENDBLK (Обработка событий). Установить параметр Final simulation time = 4.



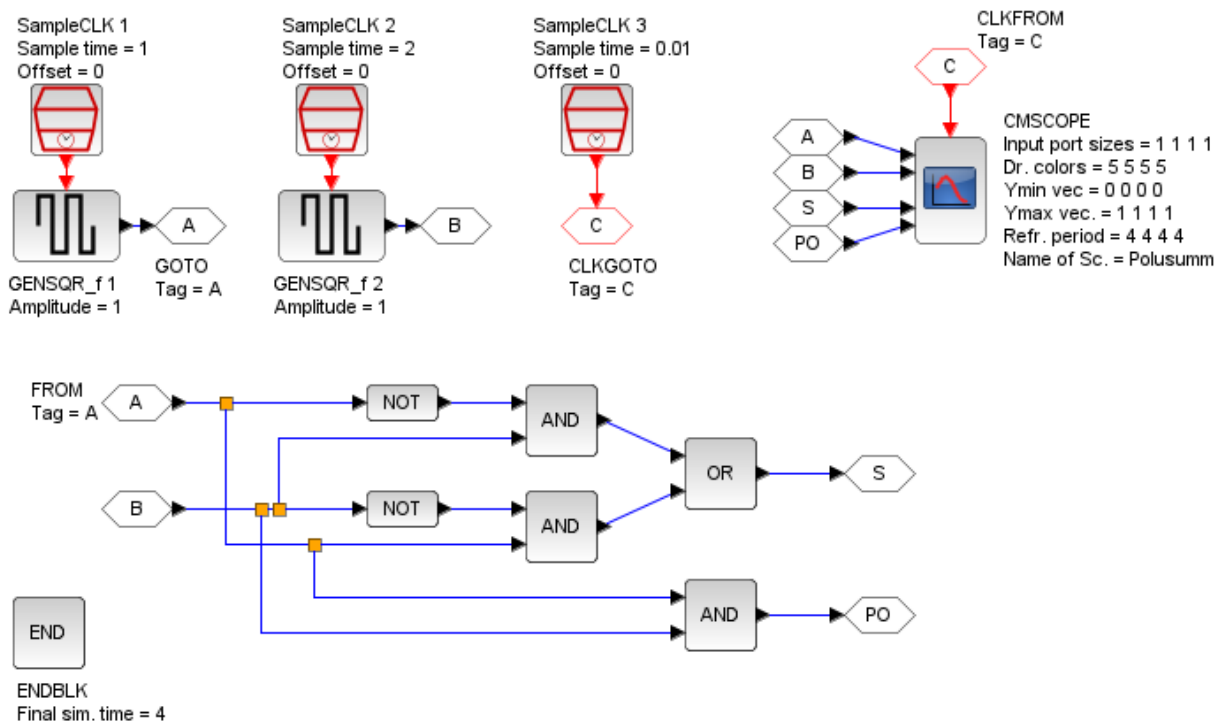


Рис. 2.1. Модель двоичного одноразрядного полусумматора в Xcos

- Добавить два блока генератора прямоугольных импульсов GENSQR\_f (Источники сигналов...). Амплитуда обоих генераторов должна быть равна 1.
- На тактовый (красный) вход первого генератора прямоугольных импульсов установить тактовый генератор SampleCLK (Источники сигналов...) с параметрами Sample time = 1 и Offset = 0. Выход первого генератора подключить к тоннелю GOTO (Маршрутизация сигналов) с тегом «А».
- На тактовый (красный) вход второго генератора прямоугольных импульсов установить тактовый генератор SampleCLK (Источники сигналов...) с параметрами Sample time = 2 и Offset = 0. Выход второго генератора подключить к тоннелю GOTO (Маршрутизация сигналов) с тегом «В».
- Добавить тактовый генератор SampleCLK (Источники сигналов...) с параметрами Sample time = 0.01 и Offset = 0. Этот генератор будет управлять осциллографом. Выход тактового генератора подключить к туннелю тактовых сигналов CLKGOTO (Маршрутизация сигналов) с тегом «С».
- Построить схему двоичного одноразрядного полусумматора, используя блоки логических элементов LOGICAL\_OP (Общепотребительные блоки). Тип блока и число входов указывается в его параметрах. При настройке блоков NOT необходимо указать число входов 1. В качестве входов полусумматора использовать блоки выхода туннеля FROM (Маршрутизация сигналов) с тегами «А» и «В», как показано на рис. 2.1. Выходы полусумматора подключить к туннелям GOTO с тегами «S» (бит суммы) и «PO» (бит переноса).

- Добавить многовходовый осциллограф CMSCOPE (Регистрирующие устройства). Задать параметры: Input ports sizes = 1 1 1; Drawing colors = 5 5 5 5; Ymin vector = 0 0 0 0; Ymax vector = 1 1 1 1; Refresh period = 4 4 4 4; Name of Scope = Polusumm. На тактовый вход осциллографа подключить тоннель CLKFROM (Маршрутизация сигналов) с тегом «С». На входы данных подать тоннели FROM с тегами «А», «В», «S» и «PO» как показано на рис. 2.1.

2. Запустить моделирование: «Моделирование» — «Запустить». Сравнить полученный график с таблицей истинности одноразрядного полусумматора. Графики отрисовываются в том же порядке, что и подключенные входы данных.

3. Экспортировать для отчета схему устройства и график. «Файл» — «Экспортировать».

### 2.4.2. Построение генератора случайных бит

Построить генератор случайных битовых элементов на основе генератора случайных чисел — ГСЧ (рис. 2.2).

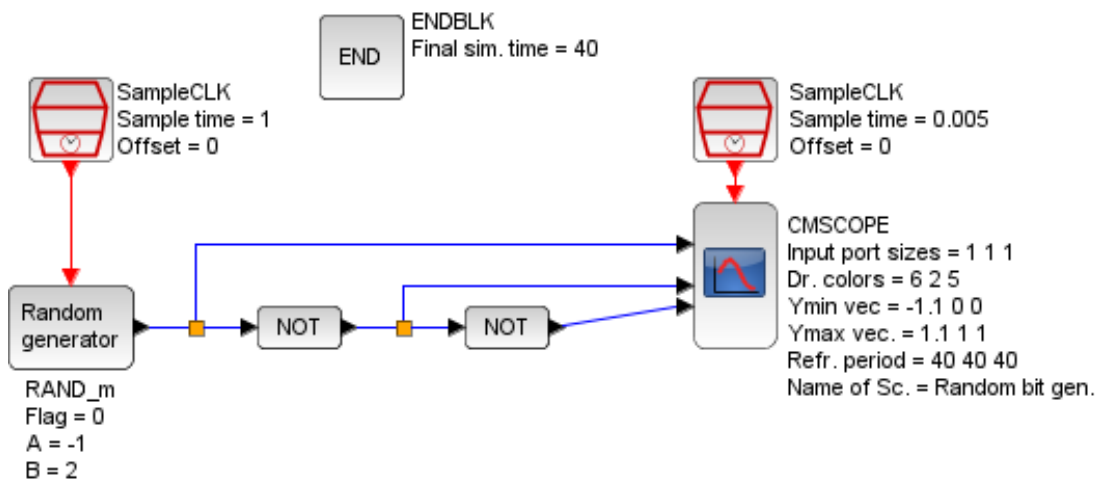


Рис. 2.2. Генератор случайных битовых элементов на основе генератора случайных чисел

1. Построить схему по образцу рис. 2.2.

- Добавить на рабочее поле блок завершения симуляции ENDBLK. Установить параметр Final simulation time = 40.

- Добавить блок ГСЧ RAND\_m (Источники сигналов. . .). Параметры: Flag = 0; A = -1; B = 2.

- На тактовый (красный) вход ГСЧ установить тактовый генератор SampleCLK с параметрами Sample time = 1 и Offset = 0.

- К выходу ГСЧ подключить последовательно два инвертора (NOT), используя блоки логических элементов LOGICAL\_OP.

- Добавить многовходовый осциллограф CMSCOPE. Задать параметры: Input ports sizes = 1 1 1; Drawing colors = 6 2 5; Ymin vector = -1.1 0 0;

Ymax vector = 1.1 1 1; Refresh period = 40 40 40; Name of Scope = Random bit gen. На тактовый вход осциллографа подключить тактовый генератор SampleCLK с параметрами Sample time = 0.005 и Offset = 0.

- На входы осциллографа подключить последовательно: выход ГСЧ, выход первого инвертора, выход второго инвертора.
- 2. Запустить моделирование: «Моделирование» — «Запустить».
- 3. Экспортировать для отчета схему устройства и график. «Файл» — «Экспортировать».
- 4. Сделать вывод о принципе работы полученного генератора случайных бит.

### 2.4.3. Суммирование сигналов

Построить схему, суммирующую сигналы от двух генераторов синусоидальных сигналов (рис. 2.3). Научиться использовать мультиплексор для построения графиков на одноходовом осциллографе.

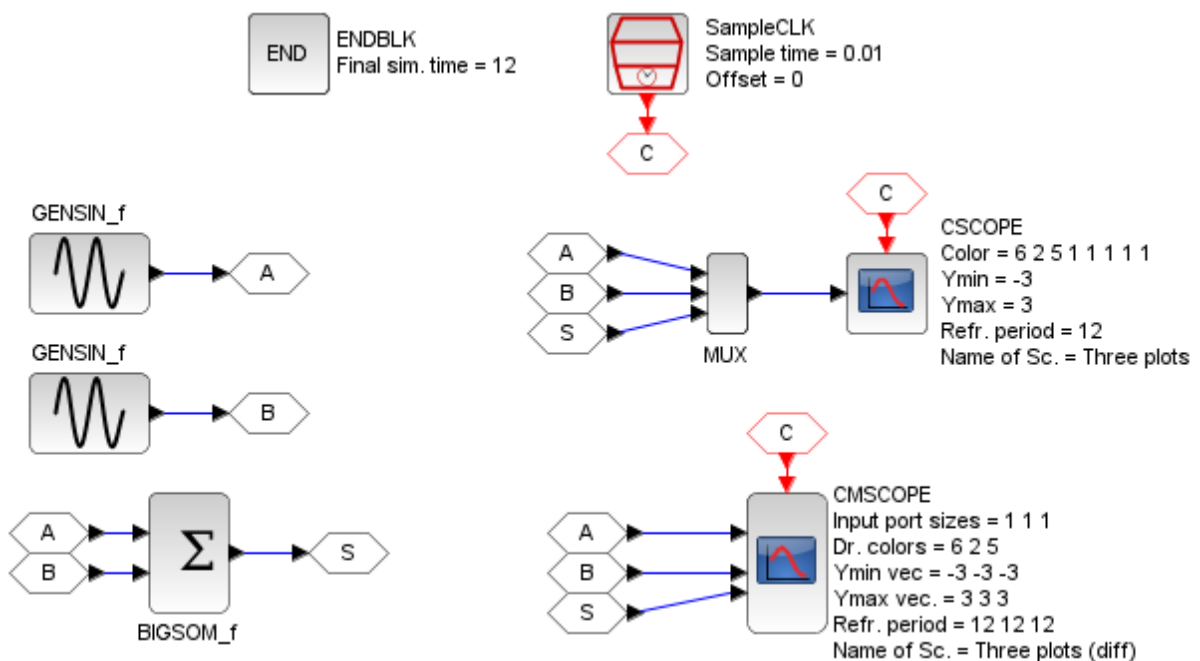


Рис. 2.3. Схема суммирования сигналов от двух генераторов синусоидальных сигналов

1. Построить схему по образцу рис. 2.3.
- Добавить на рабочее поле блок завершения симуляции ENDBLK. Установить параметр Final simulation time = 12.
- Добавить два блока генераторов синусоидальных сигналов GENSIN\_f (Источники сигналов...). Параметры первого: Амплитуда = 1. Частота = 3. Фаза = 0. Параметры второго: Амплитуда = 2. Частота = 7. Фаза =  $\pi/6$ .
- Выходы генераторов подать на сумматор BIGSOM\_f (Математические операции).

- Добавить многовходовый осциллограф CMSCOPE. Задать параметры: Input ports sizes = 1 1 1; Drawing colors = 6 2 5; Ymin vector = -3 -3 -3; Ymax vector = 3 3 3; Refresh period = 12 12 12; Name of Scope = Three plots (diff). На тактовый вход осциллографа подключить тактовый генератор SampleCLK с параметрами Sample time = 0.01 и Offset = 0.

- На входы многовходового осциллографа подключить: выход первого генератора, выход второго генератора, выход сумматора.

- Добавить одновходовый осциллограф CSCOPE. Задать параметры: Color = 6 2 5 1 1 1 1 1; Ymin = -3; Ymax = 3; Refresh period = 12; Name of Scope = Three plots. На тактовый вход осциллографа подключить тактовый генератор SampleCLK с параметрами Sample time = 0.01 и Offset = 0.

- На входы одновходового осциллографа подключить через мультиплексор MUX (Маршрутизация сигналов): выход первого генератора, выход второго генератора, выход сумматора.

2. Запустить моделирование: «Моделирование» — «Запустить».

3. Экспортировать для отчета схему устройства и графики. «Файл» — «Экспортировать».

## **2.5. Порядок защиты практической работы**

Защита работы может осуществляться одним из нижеперечисленных способов или их сочетанием на усмотрение преподавателя.

1. Устный ответ по теме работы.
2. Тестирование по теме работы
3. Задача по теме работы.
4. Иные варианты на усмотрение преподавателя.

### 3. Практическая работа. Изучение принципа работы цифрового скремблера/дескремблера

#### 3.1. Цель работы

Изучить общие принципы работы цифрового скремблера/дескремблера. Научиться строить схемы скремблеров/дескремблеров разных типов.

#### 3.2. Рекомендуемая литература

1. Скремблер [электронный ресурс] // Википедия : [сайт]  
URL: <https://ru.wikipedia.org/wiki/Скремблер>.
2. Скремблеры [электронный ресурс] // CIT Forum : [сайт]  
URL: [http://citforum.ru/internet/infsecure/its2000\\_15.shtml](http://citforum.ru/internet/infsecure/its2000_15.shtml)

#### 3.3. Порядок выполнения задания

Задание выполняется каждым учащимся индивидуально. По результатам выполнения работы должен быть написан отчет.

Отчёт формируется в рукописном или печатном виде.

Таблица 3.1

Варианты задания (указаны согласно номеру студента в журнале)

№ вар.	$L^{[ss]}$	$R_1^{[ss]}$	$I_{2-10}^{[inf]}$	$P_1^{[add]}$	$P_2^{[add]}$
1	13	7	92766537	$x^4 + x^2 + 1$	$x^8 + x^4 + x^3 + x^2 + 1$
2	13	11	94534225	$x^4 + x^3 + x^2 + 1$	$x^8 + x^5 + x^3 + x^1 + 1$
3	13	10	83656281	$x^4 + x^3 + x^1 + 1$	$x^8 + x^5 + x^3 + x^2 + 1$
4	13	9	84680943	$x^4 + x^2 + x^1 + 1$	$x^8 + x^6 + x^3 + x^2 + 1$
5	13	8	96802547	$x^4 + x^2 + 1$	$x^8 + x^6 + x^5 + x^1 + 1$
6	13	6	97889363	$x^4 + x^3 + x^2 + 1$	$x^8 + x^6 + x^5 + x^2 + 1$
7	13	5	86563629	$x^4 + x^3 + x^1 + 1$	$x^8 + x^6 + x^5 + x^3 + 1$
8	13	4	97553893	$x^4 + x^2 + x^1 + 1$	$x^8 + x^6 + x^5 + x^4 + 1$
9	13	3	96739033	$x^4 + x^2 + 1$	$x^9 + x^4 + x^3 + x^1 + 1$
10	13	2	94673925	$x^4 + x^3 + x^2 + 1$	$x^9 + x^5 + x^3 + x^2 + 1$
11	14	12	84673907	$x^4 + x^3 + x^1 + 1$	$x^9 + x^5 + x^4 + x^1 + 1$
12	14	11	86789093	$x^4 + x^2 + x^1 + 1$	$x^8 + x^7 + x^2 + x^1 + 1$
13	14	10	97653899	$x^4 + x^2 + 1$	$x^8 + x^7 + x^3 + x^2 + 1$
14	14	9	86764349	$x^4 + x^3 + x^2 + 1$	$x^8 + x^7 + x^5 + x^3 + 1$
15	14	8	87634295	$x^4 + x^3 + x^1 + 1$	$x^8 + x^7 + x^6 + x^1 + 1$
16	14	7	90773625	$x^4 + x^2 + x^1 + 1$	$x^9 + x^6 + x^4 + x^3 + 1$
17	14	6	86643999	$x^4 + x^2 + 1$	$x^9 + x^6 + x^5 + x^3 + 1$
18	14	5	88443773	$x^4 + x^3 + x^2 + 1$	$x^9 + x^7 + x^2 + x^1 + 1$
19	14	4	89942473	$x^4 + x^3 + x^1 + 1$	$x^9 + x^7 + x^4 + x^2 + 1$
20	14	3	98743663	$x^4 + x^2 + x^1 + 1$	$x^9 + x^7 + x^5 + x^1 + 1$
21	12	10	97274925	$x^4 + x^2 + 1$	$x^9 + x^7 + x^5 + x^2 + 1$
22	12	9	92837647	$x^4 + x^3 + x^2 + 1$	$x^9 + x^7 + x^6 + x^4 + 1$

Варианты задания (указаны согласно номеру студента в журнале)

№ вар.	$L^{[ss]}$	$R_1^{[ss]}$	$I_{2-10}^{[inf]}$	$P_1^{[add]}$	$P_2^{[add]}$
23	12	8	87662493	$x^4 + x^3 + x^1 + 1$	$x^9 + x^8 + x^4 + x^1 + 1$
24	12	7	87234227	$x^4 + x^2 + x^1 + 1$	$x^9 + x^8 + x^4 + x^2 + 1$
25	12	6	98236723	$x^4 + x^2 + 1$	$x^9 + x^8 + x^5 + x^1 + 1$
26	12	5	87236729	$x^4 + x^3 + x^2 + 1$	$x^9 + x^8 + x^5 + x^4 + 1$
27	12	4	89236243	$x^4 + x^3 + x^1 + 1$	$x^9 + x^8 + x^6 + x^5 + 1$
28	12	3	87234627	$x^4 + x^2 + x^1 + 1$	$x^9 + x^8 + x^7 + x^2 + 1$
29	11	8	95253793	$x^4 + x^2 + 1$	$x^9 + x^7 + x^2 + x^1 + 1$
30	11	7	97235463	$x^4 + x^3 + x^2 + 1$	$x^8 + x^6 + x^5 + x^3 + 1$

### 3.3.1. Самосинхронизирующиеся скремблеры

1. Выбрать из табл. 3.1 исходные данные для расчета.
2. Для заданных параметров (длина регистра  $L^{[ss]}$  и разряды регистра  $R_1^{[ss]}$  и  $R_2^{[ss]} = L^{[ss]}$ , охваченные обратной связью) нарисовать схемы самосинхронизирующегося скремблера и соответствующего ему дескремблера.
3. Передать через скремблер двоичную информационную комбинацию  $I_{2-10}^{[inf]}$  длиной 32 разряда. Комбинация задана в табл. 3.1 в двоично-десятичном виде. Процедуру работы скремблера (состояния ячеек регистра  $r_i$ ) и результат записать в виде табл. 3.2.

Таблица 3.2

Форма записи процедуры работы скремблера

Такт	IN	$r_1$	$r_2$	$r_3$	...	$r_{L-1}$	$r_L$	$r_{out}$	OUT
1					...				
2					...				
...					...				
31					...				
32					...				

4. Получившийся результат передать через схему дескремблера. Процедуру работы дескремблера (состояния ячеек регистра  $r_i$ ) и результат записать в виде табл. 3.2. Убедиться, что результат соответствует заданной информационной комбинации.
5. Внести одиночную ошибку в результат скремблирования и передать комбинацию с ошибкой через схему дескремблера. Процедуру работы дескремблера (состояния ячеек регистра  $r_i$ ) и результат записать в виде табл. 3.2. Сравнить результат с исходной информационной комбинацией. Сделать выводы по полученным результатам.

### 3.3.2. Аддитивные скремблеры

1. Выбрать из табл. 3.1 исходные данные для расчета.
2. Для заданного полинома  $P_1^{[add]}$  нарисовать схему аддитивного скремблера/дескремблера.
3. Проинициализировать регистр скремблера  $P_1^{[add]}$  различными двоичными комбинациями и нарисовать диаграмму состояний и переходов между ними с указанием полученных циклов. Состояния и переходы между ними оформить в виде табл. 3.3 и в виде диаграммы по образцу, приведенному в лекциях.

Таблица 3.3

Форма записи состояний работы скремблера

Состояние	$r_1$	$r_2$	$r_3$	$r_4$
1				
2				
...				
15				
16				

4. Для заданного неприводимого полинома  $P_2^{[add]}$  построить схему аддитивного скремблера/дескремблера.
5. Передать через скремблер информационную комбинацию  $I_{2-10}^{[inf]}$  длиной 32 разряда. Комбинация задана в табл. 3.1 в двоично-десятичном виде. Процедуру работы скремблера и результат записать в виде табл. 3.2.
6. Получившийся результат передать через схему дескремблера. Процедуру работы дескремблера и результат записать в виде табл. 3.2. Убедиться, что результат соответствует заданной информационной комбинации.
7. Внести одиночную ошибку в результат скремблирования и передать комбинацию с ошибкой через схему дескремблера. Процедуру работы дескремблера и результат записать в виде табл. 3.2. Сравнить результат с исходной информационной комбинацией. Сделать выводы по полученным результатам.

### 3.4. Порядок защиты практической работы

Защита работы может осуществляться одним из нижеперечисленных способов или их сочетанием на усмотрение преподавателя.

1. Устный ответ по теме работы.
2. Тестирование по теме работы
3. Задача по теме работы.
4. Иные варианты на усмотрение преподавателя.

## 4. Построение цифрового скремблера/дескремблера в симуляторе Logisim

### 4.1. Цель работы

Научиться строить схемы скремблеров/дескремблеров разных типов в симуляторе Logisim.

### 4.2. Рекомендуемая литература

1. Скремблер [электронный ресурс] // Википедия : [сайт]  
URL: <https://ru.wikipedia.org/wiki/Скремблер>.
2. Скремблеры [электронный ресурс] // CIT Forum : [сайт]  
URL: [http://citforum.ru/internet/infsecure/its2000\\_15.shtml](http://citforum.ru/internet/infsecure/its2000_15.shtml)
3. Logisim: Документация // Официальный сайт Logisim : [сайт].  
URL: <http://www.cburch.com/logisim/ru/docs.html>

### 4.3. Порядок выполнения задания

Задание выполняется каждым учащимся индивидуально. По результатам выполнения работы должен быть сформирован отчет.

Отчёт формируется в электронном виде в формате PDF.

#### 4.3.1. Самосинхронизирующиеся скремблеры

1. Выбрать из табл. 3.1 исходные данные для расчета.
2. Для заданных параметров (длина регистра  $L^{[ss]}$  и разряды регистра  $R_1^{[ss]}$  и  $R_2^{[ss]} = L^{[ss]}$ , охваченные обратной связью) построить в симуляторе Logisim схему самосинхронизирующегося скремблера. На вход скремблера подключить сдвиговый регистр длиной 32 разряда, в который будет записываться входная двоичная информационная комбинация  $I_{2-10}^{[inf]}$ . Выход скремблера подключить к сдвиговому регистру длиной 32 разряда, в который будет записан результат скремблирования.
3. Передать через скремблер двоичную информационную комбинацию  $I_{2-10}^{[inf]}$  длиной 32 разряда. Комбинация задана в табл. 3.1 в двоично-десятичном виде. Сравнить процесс и результат работы скремблера с результатом соответствующей практической работы.
4. Построить в симуляторе Logisim соответствующую схему самосинхронизирующегося дескремблера. На вход дескремблера подключить сдвиговый регистр длиной 32 разряда, в который будет записываться скремблированная комбинация. Выход дескремблера подключить к сдвиговому регистру длиной 32 разряда, в который будет записан результат дескремблирования.
5. Передать через схему дескремблера скремблированную комбинацию. Убедиться, что результат соответствует заданной информационной комбинации.



ции. Сравнить процесс и результат работы дескремблера с результатом соответствующей практической работы.

6. Внести одиночную ошибку в результат скремблирования и передать комбинацию с ошибкой через схему дескремблера. Сравнить результат с исходной информационной комбинацией. Сделать выводы по полученным результатам.

### **4.3.2. Аддитивные скремблеры**

1. Выбрать из табл. 3.1 исходные данные для расчета.

2. Для заданного неприводимого полинома  $P_2^{[add]}$  построить в симуляторе Logisim схему аддитивного скремблера/дескремблера. На вход скремблера/дескремблера подключить сдвиговый регистр длиной 32 разряда, в который будет записываться входная комбинация. Выход скремблера/дескремблера подключить к сдвиговому регистру длиной 32 разряда, в который будет записан результат скремблирования/дескремблирования.

3. Передать через скремблер информационную комбинацию  $I_{2-10}^{[inf]}$  длиной 32 разряда. Комбинация задана в табл. 3.1 в двоично-десятичном виде. Сравнить процесс и результат работы скремблера с результатом соответствующей практической работы.

4. Получившийся результат передать через схему дескремблера. Сравнить процесс и результат работы дескремблера с результатом соответствующей практической работы. Убедиться, что результат соответствует заданной информационной комбинации.

5. Внести одиночную ошибку в результат скремблирования и передать комбинацию с ошибкой через схему дескремблера. Сравнить результат с исходной информационной комбинацией. Сделать выводы по полученным результатам.

### **4.4. Порядок защиты практической работы**

Защита работы может осуществляться одним из нижеперечисленных способов или их сочетанием на усмотрение преподавателя.

1. Устный ответ по теме работы.
2. Тестирование по теме работы
3. Задача по теме работы.
4. Иные варианты на усмотрение преподавателя.

## 5. Построение цифрового скремблера/дескремблера в симуляторе Scilab/Xcos

### 5.1. Цель работы

Научиться строить схемы скремблеров/дескремблеров разных типов в симуляторе Scilab/Xcos.

### 5.2. Рекомендуемая литература

1. Скремблер [электронный ресурс] // Википедия : [сайт]  
URL: <https://ru.wikipedia.org/wiki/Скремблер>.
2. Скремблеры [электронный ресурс] // CIT Forum : [сайт]  
URL: [http://citforum.ru/internet/infsecure/its2000\\_15.shtml](http://citforum.ru/internet/infsecure/its2000_15.shtml)
3. Справка Scilab // Официальный сайт Scilab.  
URL: [https://help.scilab.org/docs/5.5.1/ru\\_RU/index.html](https://help.scilab.org/docs/5.5.1/ru_RU/index.html)
4. Чингаева, А. М. Визуальное моделирование в Scilab: Xcos. / А. М. Чингаева. — Самара : ПГУТИ. 2012.

### 5.3. Порядок выполнения задания

Задание выполняется каждым учащимся индивидуально. По результатам выполнения работы должен быть сформирован отчет.

Отчёт формируется в электронном виде в формате PDF.

#### 5.3.1. Самосинхронизирующиеся скремблеры

1. Выбрать из табл. 3.1 исходные данные для расчета.
2. Для заданных параметров (длина регистра  $L^{[ss]}$  и разряды регистра  $R_1^{[ss]}$  и  $R_2^{[ss]} = L^{[ss]}$ , охваченные обратной связью) построить в симуляторе Xcos схемы самосинхронизирующегося скремблера и соответствующего ему дескремблера. В качестве ячеек регистра использовать элемент REGISTER (Системы с дискретным временем) длиной 1 с начальным значением 0.
3. На вход скремблера подключить генератор случайных бит (рис. 2.2). Выход скремблера подключить на вход дескремблера. Выходы генератора случайных бит, скремблера и дескремблера подключить к многовходовому осциллографу CMSCOPE.
4. Задать параметры тактовых генераторов и блока завершения симуляции ENDBLK так, чтобы в результате были построены графики исходного сигнала, скремблированного сигнала и дескремблированного сигнала на длительности 24 тактов. Осциллограф должен фиксировать отсчеты каждые 0,01 такта.
5. Запустить моделирование.

6. Экспортировать для отчета схему устройства и график. «Файл» — «Экспортировать».

7. Сравнить результат дескремблирования с исходной информационной комбинацией. Сделать выводы по полученным результатам.

### 5.3.2. Аддитивные скремблеры

1. Выбрать из табл. 3.1 исходные данные для расчета.

2. Для заданного неприводимого полинома  $P_2^{[add]}$  построить в симуляторе Xcos схему аддитивного скремблера и соответствующего ему дескремблера. В качестве ячеек регистра использовать элемент REGISTER (Системы с дискретным временем) длиной 1 с соответствующими начальными значениями.

3. На вход скремблера подключить генератор случайных бит (рис. 2.2). Выход скремблера подключить на вход дескремблера. Выходы генератора случайных бит, скремблера и дескремблера подключить к многоходовому осциллографу CMSCOPE. Для синхронизации (задержки подачи тактов) на схему дескремблера использовать параметр Offset тактового генератора дескремблера.

4. Задать параметры тактовых генераторов и блока завершения симуляции ENDBLK так, чтобы в результате были построены графики исходного сигнала, скремблированного сигнала и дескремблированного сигнала на длительности 24 тактов. Осциллограф должен фиксировать отсчеты каждые 0,01 такта.

5. Запустить моделирование.

6. Экспортировать для отчета схему устройства и график. «Файл» — «Экспортировать».

7. Сравнить результат дескремблирования с исходной информационной комбинацией. Сделать выводы по полученным результатам.

### 5.4. Порядок защиты практической работы

Защита работы может осуществляться одним из нижеперечисленных способов или их сочетанием на усмотрение преподавателя.

1. Устный ответ по теме работы.

2. Тестирование по теме работы

3. Задача по теме работы.

4. Иные варианты на усмотрение преподавателя.

**Владимиров Сергей Сергеевич**

**ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ**

**Лабораторный практикум**

Издано в авторской редакции

План изданий 201X–201X, доп. п. XXX

Подписано к печати XX.XX.XXXX  
Объем X,XX печ. л. Тираж XXX экз. Заказ XXX

Редакционно-издательский отдел СПбГУТ  
193232 СПб., пр. Большевиков, 22  
Отпечатано в СПбГУТ