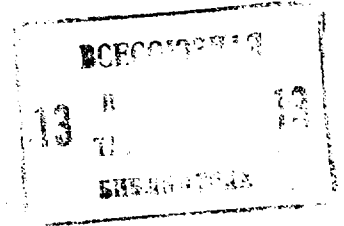




ГОСУДАРСТВЕННЫЙ КОМИТЕТ СССР  
ПО ДЕЛАМ ИЗОБРЕТЕНИЙ И ОТКРЫТИЙ

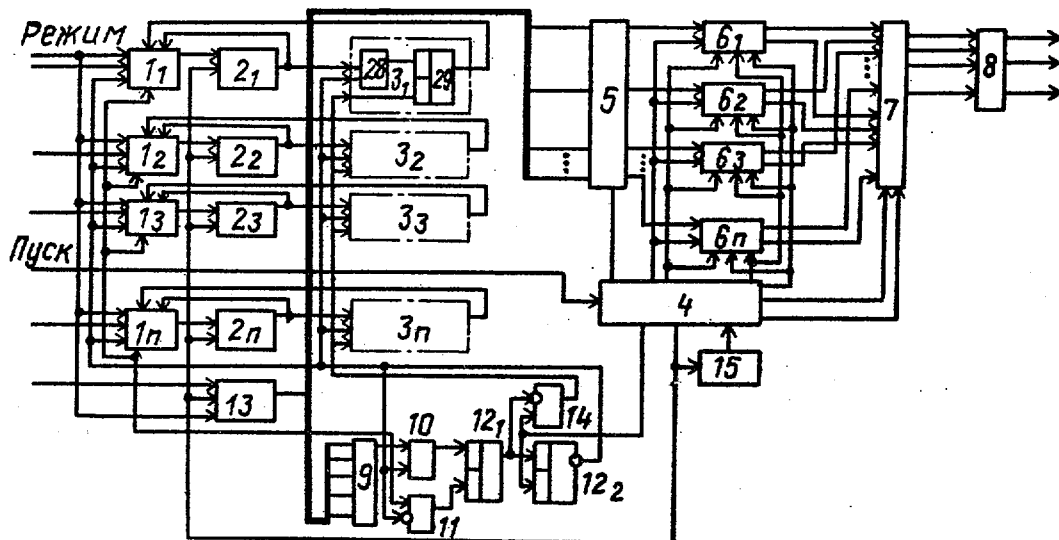


# ОПИСАНИЕ ИЗОБРЕТЕНИЯ К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

- (21) 3808996/24-24
- (22) 02.11.84
- (46) 15.05.87. Бюл. № 18
- (71) Минский радиотехнический институт
- (72) М.А.Орлов, Ю.П.Попов,  
Л.А.Смирнова и А.В.Силин
- (53) 681.333(088.8)
- (56) Авторское свидетельство СССР  
№ 1049904, кл. G 06 F 7/58, 1982.  
Авторское свидетельство СССР  
№ 1007104, кл. G 06 F 7/58, 1981.

(54) ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ  
 (57) Изобретение относится к вычислительной технике и может быть использовано при моделировании случайных процессов. Задачей, решаемой изобре-

тением, является генерирование много-разрядных случайных чисел с требуемым законом распределения. Цель изобретения - повышение быстродействия. Цель достигается за счет введения новых функциональных связей и блоков. Генератор содержит блоки 1 перезаписи, группу 2 регистров, блоки контроля 3, блоки сравнения 6, блок 5 элементов И, коммутатор 7, блок шифрации 8, сумматор по модулю два 9, два триггера 12, регистр контроля 13, элементы И 10, 11, 14, генератор равномерно распределенных чисел 15, блок управления 4. Одним из преимуществ генератора является введение в его структуру средств контроля и самовосстановления одиночных сбоев. 4 ил.



Фиг. 1

Изобретение относится к вычислительной технике и может быть использовано при моделировании случайных процессов.

Цель изобретения - повышение быстродействия генератора.

На фиг.1 представлена структурная схема генератора случайных чисел; на фиг.2 - схема блока перезаписи; на фиг.3 - схема блока сравнения; на фиг.4 - схема блока управления.

Генератор случайных чисел (фиг.1) содержит блоки  $1_1 - 1_n$  перезаписи, группу регистров  $2_1 - 2_n$ , блоки  $3_1 - 3_n$  контроля, блок 4 управления, блок 5 элементов И, блоки  $6_1 - 6_n$  сравнения, коммутатор 7, блок 8 шифрации, сумматор 9 по модулю два, два элемента И 10 и 11, два триггера  $12_1$  и  $12_2$ , регистр 13 контроля, элемент И 14, генератор 15 равномерно распределенных чисел.

Блок 1 перезаписи (фиг.2) содержит элемент И 16 первой группы, элемент И 17 второй группы, сумматор 18 по модулю два группы, элемент ИЛИ 19 группы и элемент 2И-ИЛИ 20 группы.

Блок 6<sub>i</sub> сравнения (фиг.3) содержит элементы И  $21_{2j-1}$  и  $21_{2j}$  четвертой группы, RS-триггеры  $22_{2j-1}$  и  $22_{2j}$  группы.

Блок 4 управления (фиг.4) содержит генератор 23 импульсов, регистр 24 сдвига, семь элементов ИЛИ  $25_1 - 25_7$ , девять элементов И  $26_1 - 26_9$  и одновибратор 27.

Блок  $3_1 - 3_n$  контроля содержит элемент И 28 третьей группы и счетный триггер 29 группы.

Рассмотрим работу генератора случайных чисел.

Перед началом работы производится запись информации в регистры 2 группы. Для этого на вход задания режима генератора подается нулевой сигнал, который разрешает запись информации в регистры 2 группы. За  $(m+1)$  тактов сдвига ( $m$  - разрядность кода вероятностей,  $(m+1)$ -й разряд - контрольный) происходит заполнение регистров 2. Затем на вход задания режима генератора подается единичный сигнал и регистры 2 группы начинают функционировать как циклические.

Последовательность тактовых импульсов, обеспечивающих синхронную работу устройства, вырабатывает блок 4 управления, который функционирует

следующим образом. По сигналу "Пуск" сбрасывается регистр 24, который организован как циклический сдвиговый регистр. Этот же сигнал запускает генератор 23 импульсов, проходит через элементы ИЛИ  $25_6$  и  $26_6$  и производит начальный сброс RS-триггеров 22 группы блоков 6 сравнения. По этому сигналу с задержкой  $\hat{c}$ , необходимой для сброса RS-триггеров 22 группы, одновибратор 27 формирует единичный сигнал начальной установки, который через первый элемент ИЛИ  $25_1$  поступает на информационный вход регистра 24 и вторым импульсом генератора 23 записывается в младший разряд регистра 24. Далее в течение всего функционирования устройства регистр 24 работает как циклический сдвиговый регистр, в котором перемещается единица.

С помощью элементов ИЛИ 25 вырабатывается разрешение на прохождение импульсов генератора 23 через соответствующие элементы И 26.

После окончания установочных операций начинается функционирование устройства, т.е. сравнение равномерно распределенного числа (РРЧ) с кодами вероятностей функции распределения. В каждый такт работы устройства происходит сравнение одного разряда РРЧ с соответствующими разрядами кодов вероятностей.

К началу цикла сравнения на выходах регистров 2 группы устанавливаются старшие разряды кодов вероятностей.

Блок 4 управления на первых  $n$  тактах обеспечивает выработку  $n$  синхронизирующих импульсов, которые сдвигают информацию в регистрах 2 группы и в регистре 13 (с выхода девятого элемента И  $26_9$  блока 4 управления), а также синхронизацию  $j$ -х RS-триггеров группы  $22_k$  ( $k = 1, 3, 5, \dots, 2n-1$ ) - с выхода восьмого элемента И-26<sub>8</sub> блока 4 управления, а также  $k$ -х RS-триггеров группы  $22_k$  ( $k = 2, 4, 6, \dots, 2n$ ) - с выхода седьмого элемента И  $26_7$  блока 4 управления.

Единичный сигнал с выхода элемента ИЛИ 30<sub>5</sub> поступает на вход блока 5 элементов И и разрешает прохождение кодов вероятностей функции распределения через него, а также обеспечивает прохождение цифры РРЧ с выхода

генератора 15 на входы блоков 6 сравнения.

В каждом блоке  $6_j$  сравнения с помощью элементов И 21 четвертой группы производится операция сравнения. Если на первые входы элементов  $21_{2j-1}$  и  $21_{2j}$  поступает одинаковая информация, они вырабатывают нулевой сигнал и RS-триггеры  $22_{2j-1}$  и  $22_{2j}$  остаются в нулевом состоянии. Если разряд кода вероятности больше разряда РРЧ, то на выходе элемента  $21_{2j-1}$  появляется единичный сигнал, который устанавливает в единицу соответствующий триггер  $22_{2j-1}$ . В противном случае в единицу устанавливается RS-триггер  $22_{2j}$  группы. Поскольку операция сравнения начинается со старших разрядов, то установление в единицу одного из триггеров 22 группы означает, что в данном  $j$ -м блоке  $6_j$  сравнения операция сравнения завершена.

Цикл сравнения продолжается до тех пор, пока на выходах регистров 2 группы не появятся младшие разряды кодов вероятностей, хотя для его завершения достаточно, чтобы во всех блоках 6 сравнения сработал хотя бы один из триггеров  $22_j$  или  $22_k$ , и, соответственно, запретил срабатывание второго.

После окончания цикла сравнения информация с выходов блоков 6 сравнения поступает через коммутатор 7 на входы блока шифрации и на выход устройства.

Для контроля и самовосстановления одиночных сбоев в предлагаемом устройстве используются сумматор 9 по модулю два, а также блоки 3 контроля.

В режиме нормального функционирования информация с выходов регистров 2 группы проходит через элементы И 28 третьей группы на счетные входы триггеров 29 группы, которые определяют, является ли четным количество единиц в последовательностях, содержащихся в регистрах 2 группы (младший бит последовательности дополняет сумму его членов до четной). Одновременно с этим на каждом такте информация с выходов каждого из регистров 2 группы суммируется в блоке 9 с контрольным битом, дополняющим сумму до четной. Контрольные биты хранятся в регистре 13 и на каждом такте сдвига-

ются в соответствии с информацией регистров 2 группы.

При возникновении одиночного сбоя единичный сигнал с выхода сумматора 9 по модулю два проходит через элемент И 10 и устанавливает триггер  $12_1$ . Сигналом с выхода первого элемента И 26<sub>1</sub> блока 4 управления, возникающим по окончании цикла сравнения, единица из RS-триггера  $12_1$  переписывается в D-триггер  $12_2$ . Появление единицы в триггере  $12_2$  означает начало режима коррекции.

Если сбой одиночный, то в одном из счетных триггеров группы будет зафиксирована единица.

Далее следует цикл коррекции. В этом случае элементы И 28 третьей группы закрыты сигналом с инверсного входа триггера  $12_2$  и на счетные входы триггеров 29 группы информация не поступает. Поскольку в счетном триггере 29  $i$ -го блока контроля 3<sub>1</sub> зафиксирована единица, то на первом входе элемента И 17 второй группы блока 1<sub>1</sub> перезаписи присутствует единичный сигнал, свидетельствующий о том, что в соответствующем регистре 2 группы произошла ошибка. В момент, когда сбойный разряд поступает на выход  $i$ -го регистра 2 группы, на выходе сумматора 9 по модулю два возникает единичный сигнал, поступающий на второй вход элемента И 17 второй группы; далее он проходит через элемент И 17 и складывается сумматором 18 по модулю два группы с ошибочным битом, поступающим с выхода регистра 2 группы. Таким образом, ошибка исправляется и скорректированный бит поступает через элементы ИЛИ 19 группы и 2И-ИЛИ 20 группы на информационный вход регистра 2.

Сигнал с выхода сумматора 9 по модулю два проходит также через элемент И 11 и сбрасывает RS-триггер  $12_1$ . Очередной сигнал об окончании цикла сравнения переписывает нулевое содержимое триггера  $12_1$  в триггер  $12_2$ , и цикл коррекции заканчивается. Этот же сигнал сбрасывает счетные триггеры 29 группы.

Для генерирования случайных чисел с усеченной функцией распределения (или условных вероятностей) блок 5 элементов И может быть заменен коммутатором. При этом первые информационные входы коммутатора подключаются

к выходам регистров 2 группы, а вторые информационные входы служат в качестве входов генератора случайных чисел для занесения левой и правой границ усеченной функции распределения. В этом случае перед началом цикла сравнения информация о левой и правой границах в два такта записывается соответственно в  $j$ -е и  $k$ -е RS-триггеры 22 группы ( $j=1, 3, 5, \dots, 2n-1, k=2, 4, 6, \dots, 2n$ ). Далее следует цикл сравнения, причем окончательный результат сравнения формируется в пределах определенных ранее границ.

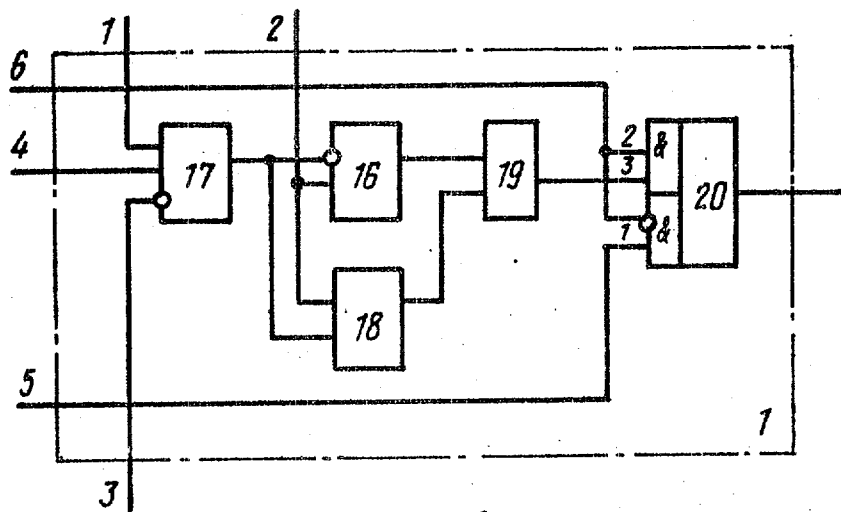
#### Ф о р м у л а и з о б р е т е н и я

Генератор случайных чисел, содержащий генератор равномерно распределенных чисел, группу регистров, блок шифрации, отличающийся тем, что, с целью повышения быстродействия, он содержит четыре группы элементов И, группу счетных триггеров, группу RS-триггеров, три элемента И, сумматор по модулю два, группу элементов 2И-ИЛИ, группу сумматоров по модулю два, группу элементов ИЛИ, регистр контроля, первый и второй триггеры, блок элементов И, коммутаторы и блок управления, который содержит генератор импульсов, регистр сдвига, семь элементов ИЛИ, одновибратор, девять элементов И, причем в блоке управления выход одновибратора соединен с первым входом первого элемента ИЛИ, выход которого соединен с информационным входом регистра сдвига, выходы разрядов с первого по  $n$ -й регистра сдвига (где  $n$  - число интервалов квантования функции распределения) соединены с одноименными входами второго, третьего, четвертого и пятого элементов ИЛИ, выход  $(n+1)$ -го разряда регистра сдвига соединен с  $(n+1)$ -м входом четвертого элемента ИЛИ, первым входом первого элемента И, выход  $(n+2)$ -го разряда регистра сдвига соединен с первым входом второго элемента И, выход  $(n+3)$ -го разряда сдвига соединен с первым входом третьего элемента И, выход  $(n+4)$ -го разряда регистра сдвига соединен с первым входом шестого элемента ИЛИ и  $(n+2)$ -ми входами второго и третьего элементов ИЛИ, выход  $(n+5)$ -го разряда регистра сдвига соединен с  $(n+3)$ -м

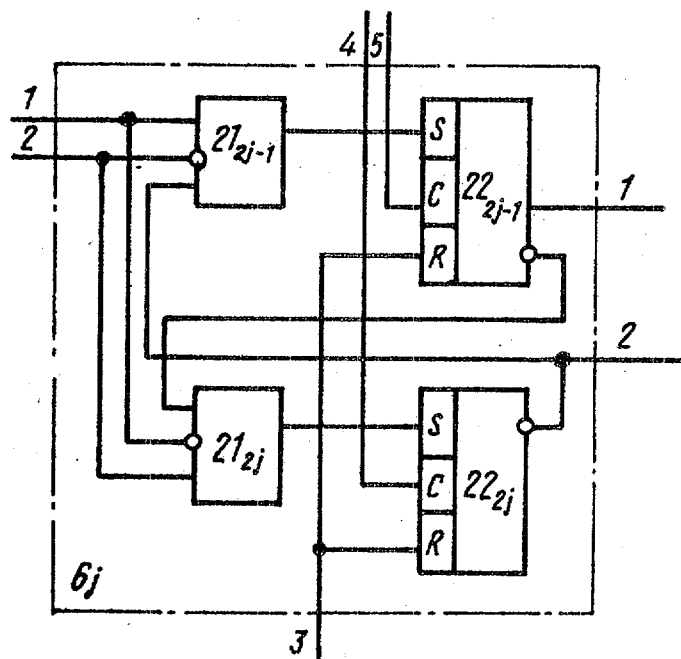
входом третьего элемента ИЛИ, выход  $(n+6)$ -го разряда регистра сдвига соединен с прямым входом четвертого элемента И,  $(n+3)$ -м входом второго элемента ИЛИ и с вторым входом первого элемента ИЛИ, инверсный вход четвертого элемента И соединен с первым входом пятого элемента И и подключен к выходу пятого элемента ИЛИ, выход шестого элемента ИЛИ соединен с первым входом шестого элемента И, выход второго элемента ИЛИ соединен с первым входом седьмого элемента И, выход третьего элемента ИЛИ соединен с первым входом восьмого элемента И, выход четвертого элемента ИЛИ соединен с первым входом девятого элемента И, выход пятого элемента И соединен с первым входом седьмого элемента ИЛИ, второй вход которого соединен с выходом четвертого элемента И, вход одновибратора соединен с входом обнуления регистра сдвига, входом запуска генератора импульсов, вторым входом шестого элемента ИЛИ, с  $(n+1)$ -ми входами второго и третьего элементов ИЛИ и является входом "Пуск" генератора случайных чисел, выход генератора импульсов соединен с вторыми входами первого, второго, третьего, шестого, седьмого, восьмого и девятого элементов И и с входом синхронизации регистра сдвига, первые прямые входы элементов 2И-ИЛИ группы и информационный вход регистра контроля подключены к разрядным входам задания закона распределения генератора, инверсные входы элементов 2И-ИЛИ группы соединены с вторыми прямыми входами элементов 2И-ИЛИ группы, с тактовым входом регистра контроля и подключены к входу задания режима генератора, выходы регистров группы и выход регистра контроля подключены к соответствующим входам сумматора по модулю два, выходы регистров группы подключены к группе информационных входов блока элементов И, выходов регистров группы соединены с прямыми входами одноименных элементов И первой группы и с первыми входами сумматоров по модулю два группы, инверсный вход каждого элемента И первой группы соединен с выходом соответствующего элемента И второй группы и вторым входом одноименного сумматора по модулю два группы, выход которого соединен с первым входом соответствующего элемента ИЛИ груп-

пы, второй вход которого соединен с выходом соответствующего элемента И первой группы, инверсные первые входы элементов И третьей группы соединены с первыми входами первого и второго элементов И, с инверсными входами элементов И второй группы и подключены к инверсному выходу D-триггера, первые прямые входы элементов И второй группы подключены к выходам соответствующих счетных триггеров группы, выход первого элемента И блока управления соединен с первым входом третьего элемента И и входом синхронизации D-триггера, вход которого соединен с выходом RS-триггера и вторым входом третьего элемента И, выход которого подключен к входам "Сброс" счетных триггеров группы, единичный и нулевой входы RS-триггера соединены с выходами соответственно первого и второго элементов И, вторые входы которых объединены и подключены к выходу сумматора по модулю два и к вторым прямым входам элементов И второй группы, выходы элементов 2И-ИЛИ группы соединены с соответствующими информационными входами регистров группы, входы синхронизации регистров группы соединены с входом синхронизации регистра контроля, входом опроса генератора равномерно распределенных чисел и подключены к выходу девятого элемента И блока управления, второй вход пятого элемента И блока управления соединен с выходом генератора равномерно распределенных чисел, выход шестого элемента И блока управления подключен к нулевым входам RS-триггеров группы, выход седьмого элемента И блока управ-

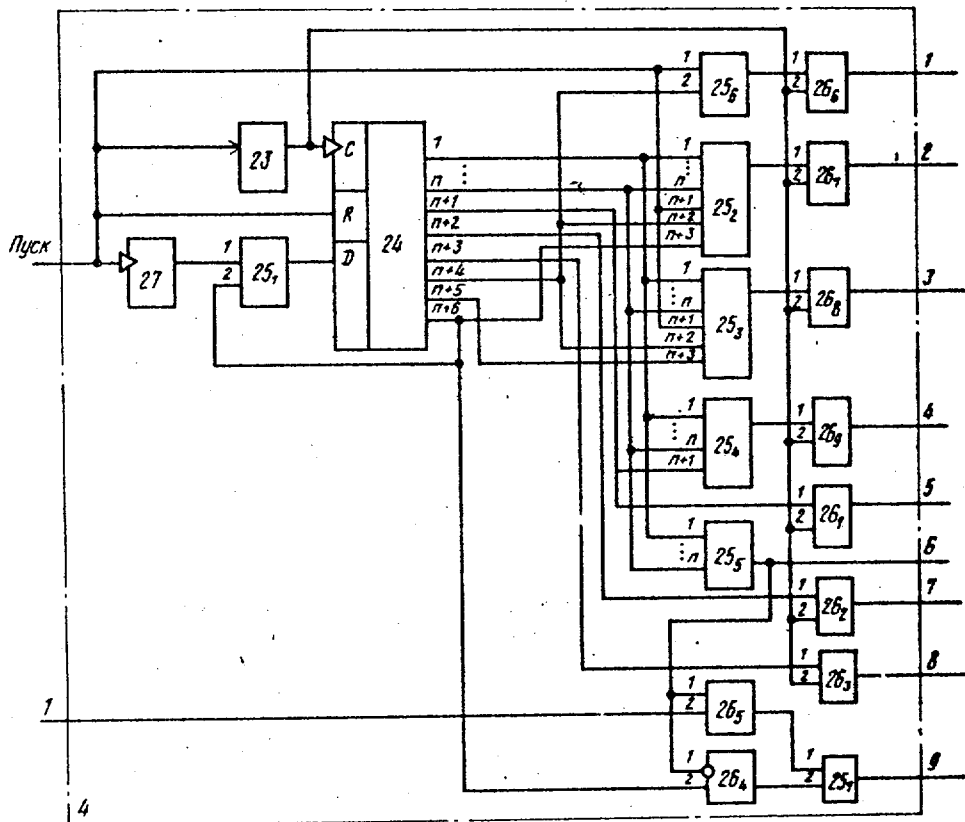
ления соединен с входами синхронизации k-х RS-триггеров группы (где  $k = 2, 4, 6, \dots, 2n$ ), выход восьмого элемента И блока управления соединен с входами синхронизации j-х RS-триггеров группы (где  $j = 1, 3, \dots, 2n-1$ ), выход седьмого элемента ИЛИ блока управления соединен с инверсными входами j-х элементов И четвертой группы и с первыми прямыми входами k-х элементов И четвертой группы, выход каждого элемента И четвертой группы подключен к единичному входу одноименного RS-триггера группы, второй прямой вход каждого (k-го элемента И четвертой группы) подключен к инверсному выходу (k-1)-го RS-триггера группы, а инверсный выход k-го RS-триггера группы соединены с вторым прямым входом (k+1)-го элемента И четвертой группы, третьи прямые входы j-х элементов И четвертой группы и инверсные входы k-х элементов И четвертой группы подключены к соответствующим k-м выходам блока элементов И, управляющий вход которого соединен с выходом пятого элемента ИЛИ блока управления, выходы второго и третьего элементов И блока управления подключены к первому и второму управляющим входам коммутатора соответственно, первая группа информационных входов которого подключена к прямым выходам j-х RS-триггеров группы соответственно, а вторая группа информационных входов коммутатора соединена с инверсными выходами k-х RS-триггеров группы соответственно, выходы коммутатора соединены с соответствующими входами блока шифрации, выход которого является выходом генератора.



Фиг. 2



Фиг. 3



Фиг. 4

Редактор М. Дылынь      Составитель И. Столяров      Техред Л. Олейник      Корректор Г. Решетник

Заказ 1892/45      Тираж 673      Подписное  
 ВНИИПИ Государственного комитета СССР  
 по делам изобретений и открытий  
 113035, Москва, Ж-35, Раушская наб., д. 4/5

Производственно-полиграфическое предприятие, г. Ужгород, ул. Проектная, 4