

АЛГОРИТМЫ ГЕНЕРАЦИИ И ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ



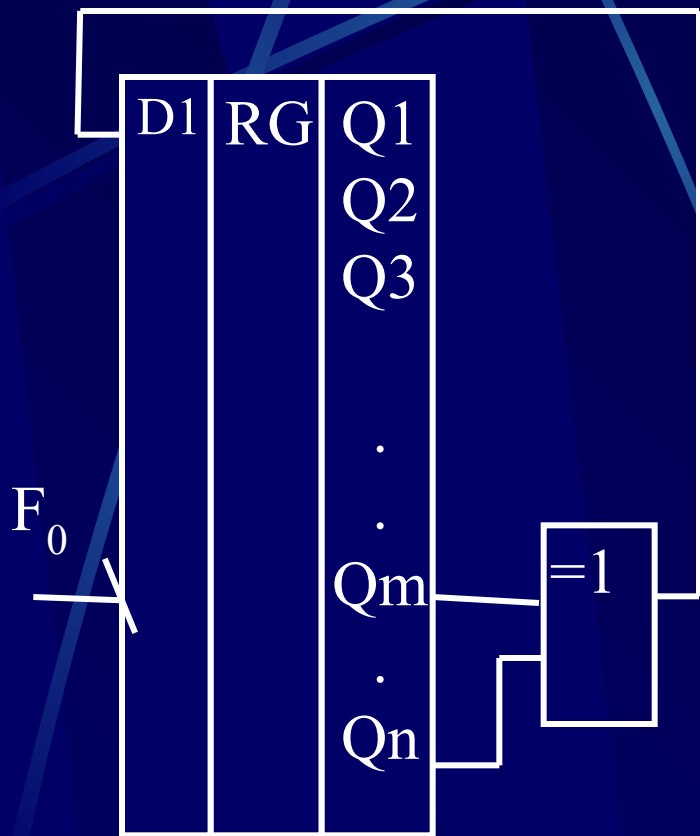
ОСНОВНЫЕ ТЕМЫ ЛЕКЦИИ

- ОТЛИЧИЯ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ
- ВЫБОР ФИЗИЧЕСКИХ ДАТЧИКОВ ШУМА
- БАЗОВАЯ МОДЕЛЬ ГЕНЕРАТОРА СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ
- ВЫРАВНИВАНИЕ ВЕРОЯТНОСТЕЙ ГЕНЕРИРУЕМЫХ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ
- МЕТОДЫ ПОВЫШЕНИЯ БЫСТРОДЕЙСТВИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ
- МЕТОДЫ ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ МЕТОДИКИ **FIPS 140-1**.

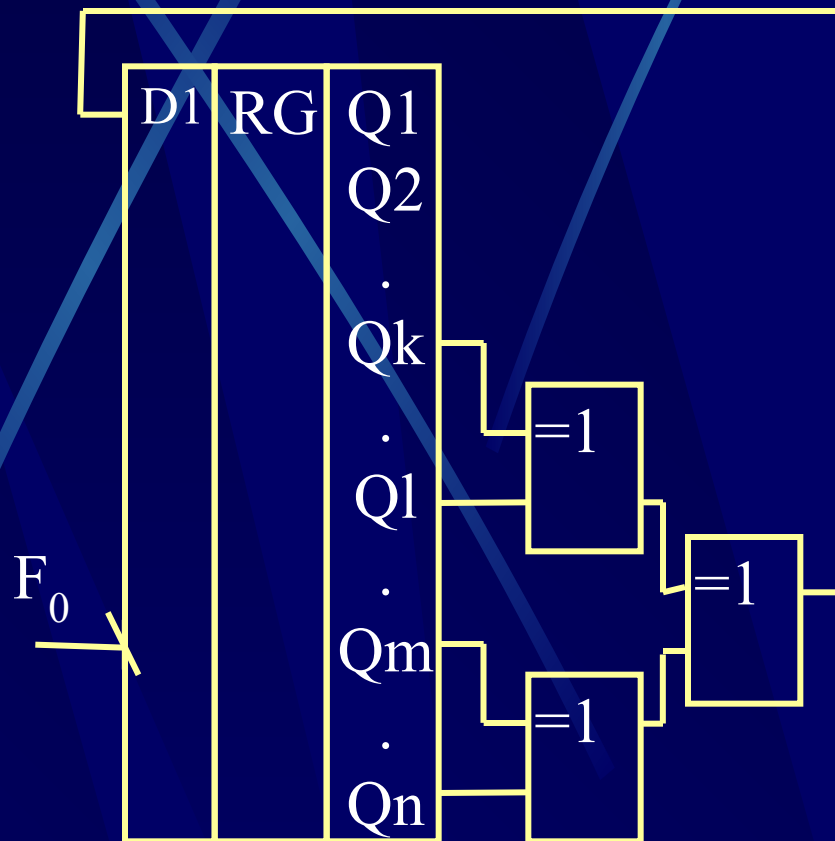
РЕАЛИЗАЦИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

- С помощью **цифровых логических схем** можно необычайно просто генерировать последовательности бит с **хорошими стохастическими свойствами**, т.е. последовательности, которые будут обладать такими же **вероятностными** и **корреляционными** свойствами, какими обладает идеальная машина для подбрасывания монеты.
- Поскольку эти последовательности генерируются стандартными элементами **детерминированной логики**, получающиеся двоичные последовательности на самом деле являются **предсказуемыми** и повторяемыми (**детерминированными**), хотя любой фрагмент такой последовательности во всех отношениях выглядит, как **случайное чередование «0» и «1»**.

- Наиболее известным (и самым простым) генератором **ПСП** является регистр сдвига с обратной связью



*Последовательный регистр
с одним отводом*



*Последовательный регистр с
тремя отводами*

- Последовательный регистр **RG** длиной «**n**» осуществляет **сдвиг хранимого кода** после каждого тактового импульса с частотой **F_0** . Входной сигнал первого триггера регистра – **D1** формируется с помощью вентиля **ИСКЛЮЧАЮЩЕЕ ИЛИ** (сумматора по модулю 2), на входы которого поступают сигналы от **m-того** и последнего (**n-того**) разрядов регистра.
- Такая схема проходит через множество состояний, которые после **K** тактов начинают **повторяться**, т.е. последовательность состояний является **циклической** с **периодом K**.

- Максимальное число возможных состояний **n-разрядного** регистра равно $K=2^n$, т.е. числу **n-битовых** двоичных комбинаций. Однако состояние «**все нули**» для этой схемы является **тупиковым**, поскольку на выходе схемы **ИСКЛЮЧАЮЩЕЕ ИЛИ** постоянно **появляются нули**, которые поступают на вход схемы и **зацикливаются**.
- Если для формирования входного сигнала использовать элемент «**ИСКЛЮЧАЮЩЕЕ ИЛИ**» с **инверсией**, то «**тупиковой**» будет комбинация – «**все единицы**».
- Таким образом, **последовательность максимальной длины**, которую может сформировать данная схема, содержит 2^n-1 бит.

- При использовании **33-х** разрядного регистра, работающего **на частоте 1 МГц**, **время цикла** будет около **2-х часов**. Время цикла **100 разрядного** регистра, работающего на частоте **10 МГц**, будет в **миллион раз больше, чем возраст Вселенной**.
- Генераторы **ПСП** на сдвигающих регистрах можно использовать для **шифрования сообщений и данных**, поскольку идентичный генератор **ПСП** на приемном конце дает **ключ к шифру**.
- **ПСП** широко используются в кодах, **обнаруживающих и исправляющих ошибки**, так как они позволяют видоизменить блоки данных таким образом, что **правильные кодовые сообщения** будут находиться друг от друга на **максимально возможном «расстоянии Хэмминга»** (измеряется числом позиций с разными данными).

СВОЙСТВА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАКСИМАЛЬНОЙ ДЛИНЫ

- В полном цикле число «1» на единицу больше, чем число «0». Добавочная «1» появляется за счет исключения состояния «все нули». При большом количестве разрядов регистра вероятности «0» и «1» практически равны (17-ти разрядный регистр будет вырабатывать 65536 «1» и 65535 «0» за один цикл);
- В одном цикле половина серий из последовательных «1» имеет длину 1, одна четвертая серий – длину 2, одна восьмая – длину 3 и т.д. Таким же свойством обладают и серии из «0» с учетом пропущенного «0». Это говорит о том, что вероятности «0» и «1» не зависят от исхода предыдущего опыта, т.е. вероятность появления «0» или «1» в следующем бите не зависит от значения предыдущего бита;

- Если последовательность полного цикла сравнить с этой же последовательностью, но циклически **сдвинутой на любое число битов** (не равное нулю или длине K), то **число несовпадений** будет на **единицу** больше, чем **число совпадений**. Научно выражаясь, **автокорреляционная функция** этой последовательности представляет собой **дельта-функцию Кронекера** при нулевой задержке и равна величине **$1/K$** при любой другой задержке.

ОСНОВНЫЕ ОТЛИЧИЯ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ ОТ СЛУЧАЙНЫХ

- Псевдослучайные числа являются **детерминированными**, то есть предсказуемыми. Зная **алгоритм формирования** и **начальное значение**, можно предсказать **все** последующие числа наперед.
- В **новом эксперименте** всегда можно повторить **предыдущий эксперимент**.
- Псевдослучайные последовательности являются **периодическими**, через известные промежутки времени они будут **точно повторяться**.

- Предельные характеристики стойкости криптографических систем достигаются в случае, если для формирования ключей, параметров и синхромаркеров используется генератор случайных последовательностей на основе **ФИЗИЧЕСКИХ ДАТЧИКОВ ШУМА** с наилучшими параметрами:

- **равновероятности,**

- **независимости** и

- **некоррелированности** на сколь угодно длинном интервале.

- Простейшие **физические датчики**, реализованные на основе случайных механических перемещений:

- **подбрасывание монеты**,
- бросание «игральных костей»,
- **наблюдения броуновского движения и др.**

обладают недостаточным быстродействием и требуют для своей реализации оптические устройства ввода результатов опытов в ЭВМ.

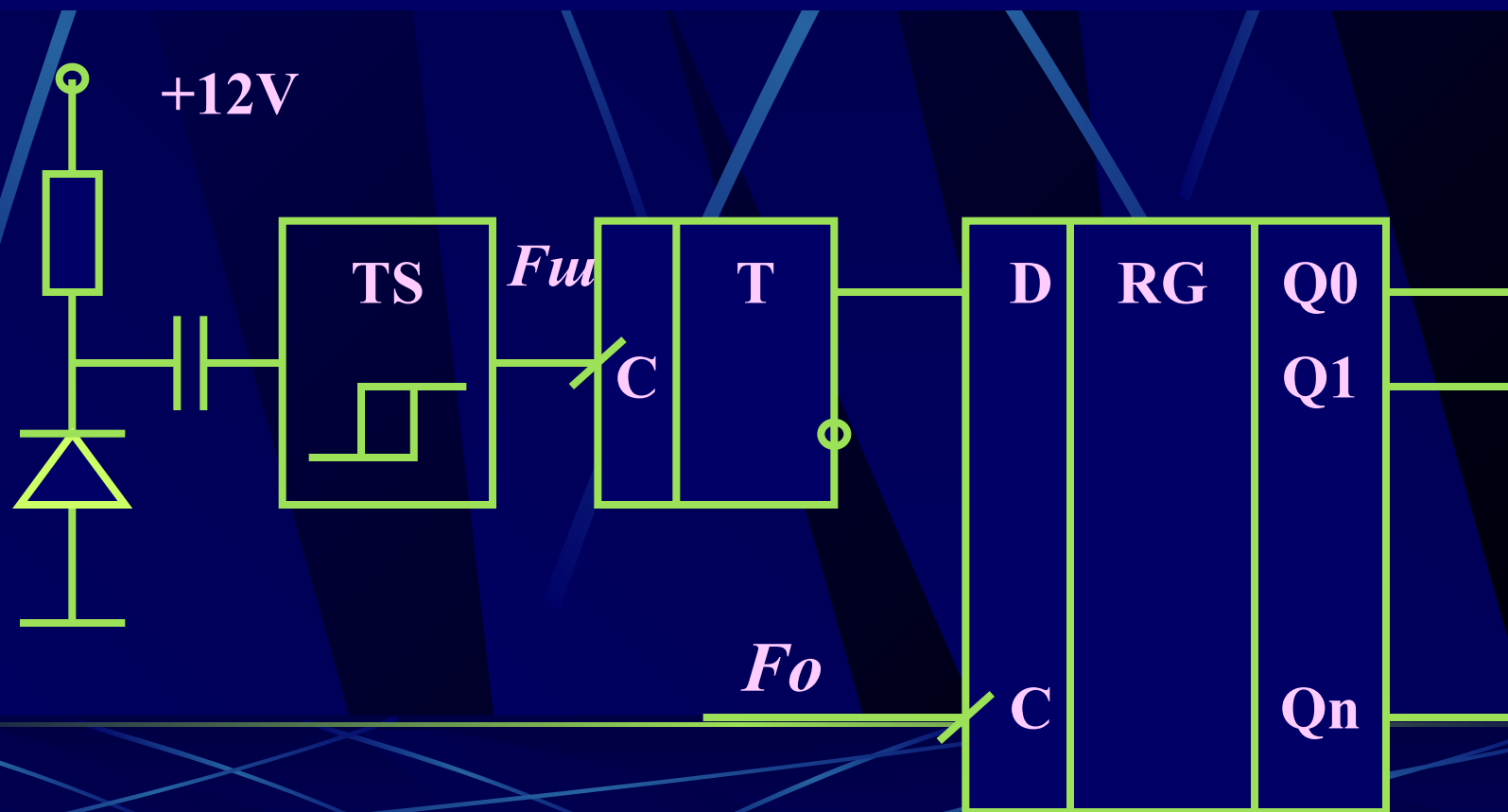
Основные датчики шума

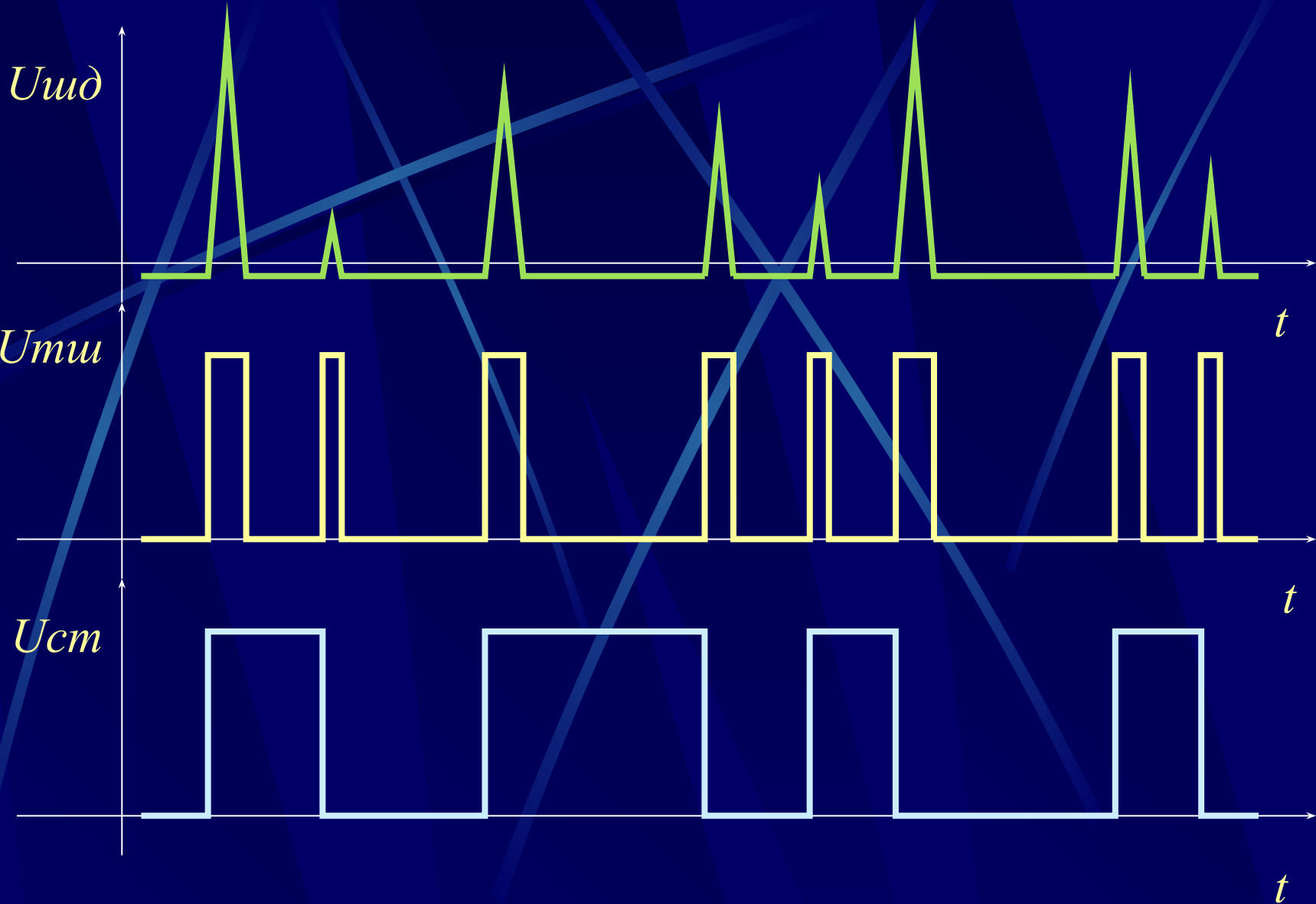
- Резисторы
- P-n-переходы
- **Диоды с Зенеровским пробоем**
- Электр. лампы
- Газоразрядные лампы
- ФЭУ
- Счетчики радиоактивности

Критерии выбора

- полоса частот случайного сигнала;
- выходное напряжение (амплитуда шума);
- потребляемая мощность;
- напряжение питания;
- массогабаритные параметры;
- надежность работы при изменении условий эксплуатации;
- экономические показатели (стоимость).

- На рис. приведена базовая схема генератора случайных последовательностей на основе физического датчика – диода с Зенеровским пробоем.
Зенеровским пробоем.

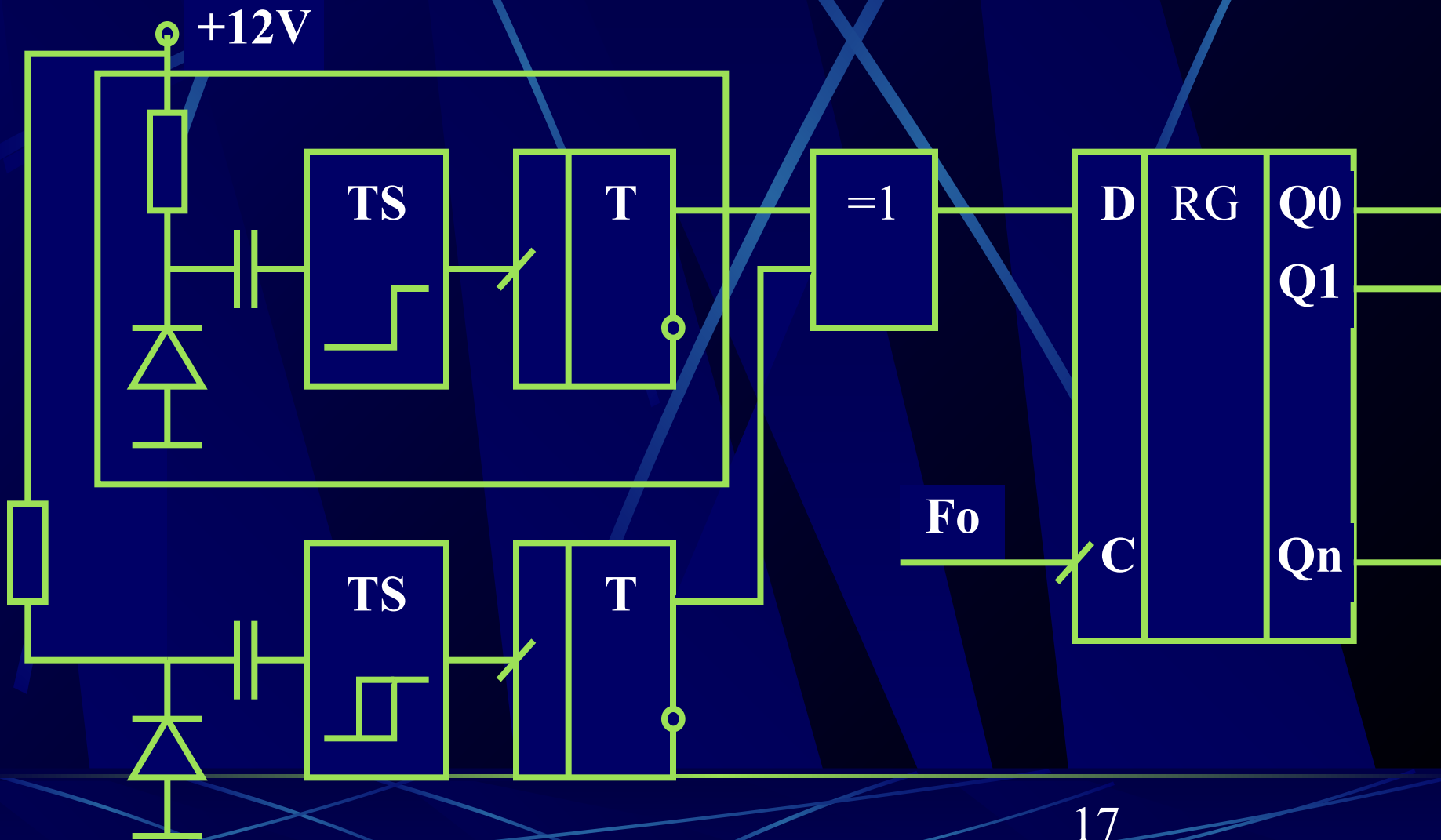


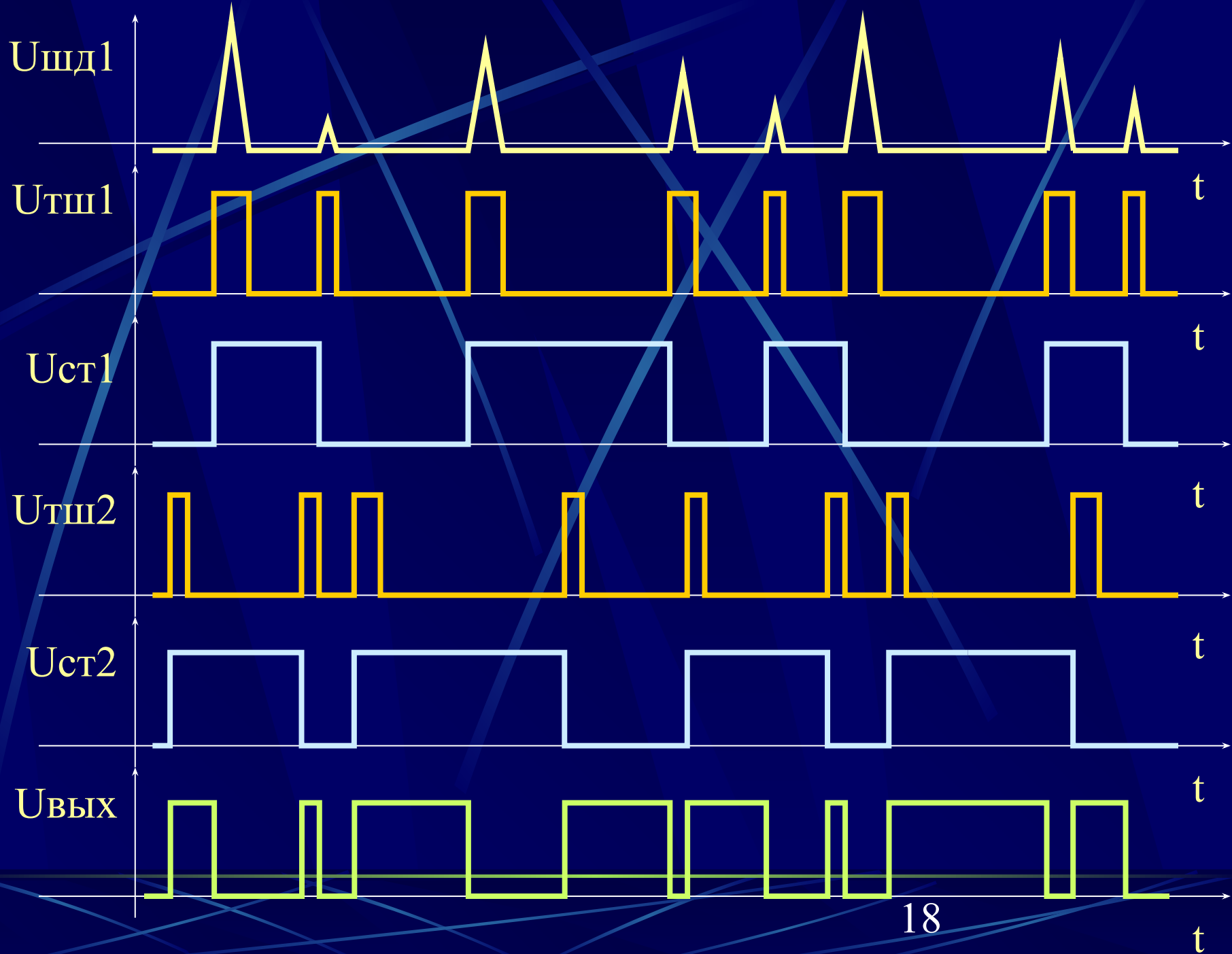


Временные диаграммы формирователя случайных битов

- Повышение эксплуатационной **надежности** канала формирования случайных битов достигается **горячим резервированием**, то есть параллельной работой нескольких каналов.
- Выходные равновероятные случайные логические сигналы всех каналов объединяются схемой **«ИСКЛЮЧАЮЩЕЕ ИЛИ»** (схемой суммирования по модулю 2) и считываются в сдвигающий регистр с частотой F_0

- Горячее резервирование генераторов случайных последовательностей

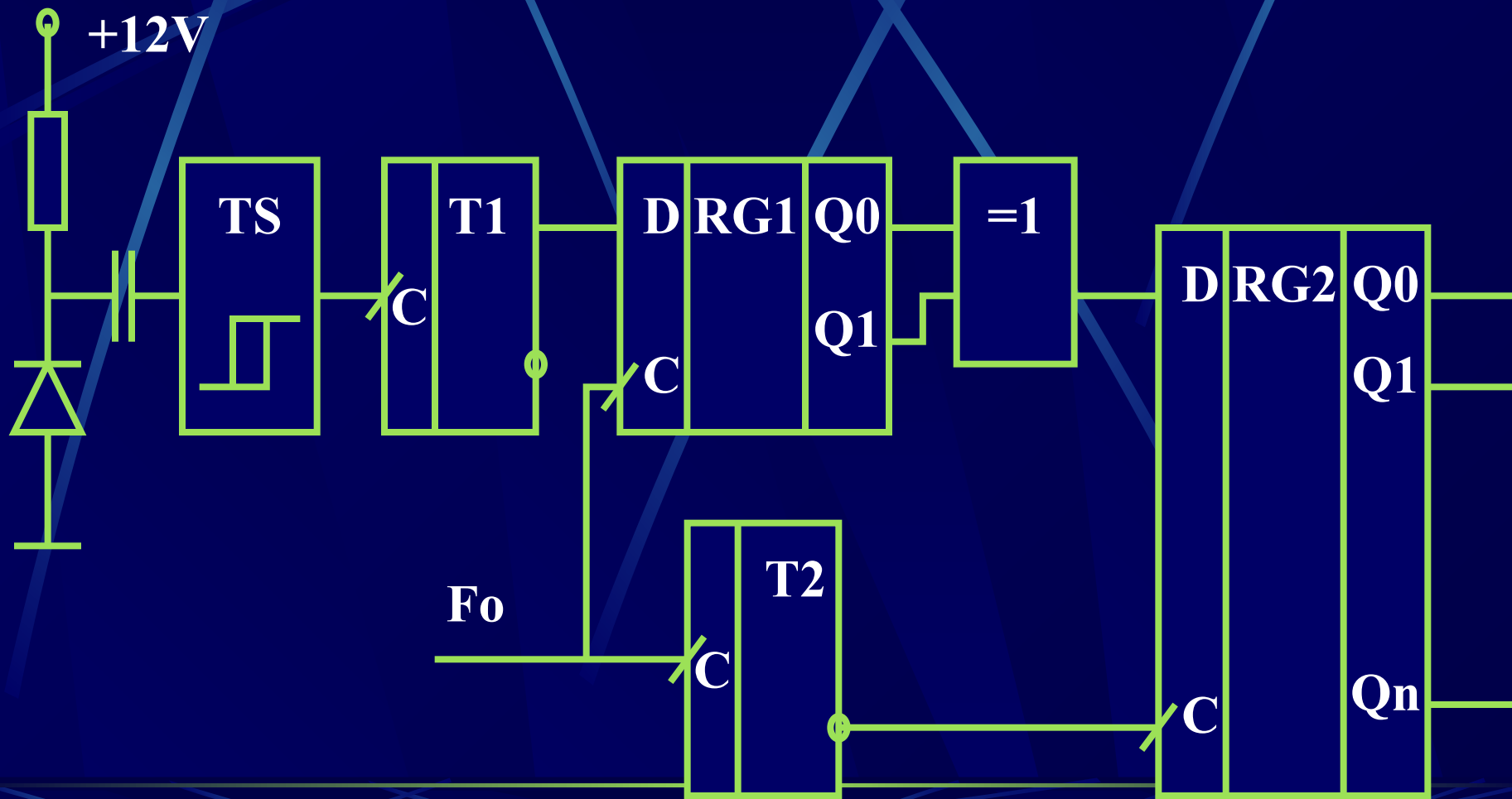




ВЫРАВНИВАНИЕ ВЕРОЯТНОСТЕЙ ГЕНЕРИРУЕМЫХ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

- Для выравнивания вероятностей из двух последовательных случайных битов на выходах дополнительного регистра формируется их логическая функция **«ИСКЛЮЧАЮЩЕЕ ИЛИ»**.
- Вероятность единичного формируемого бита **на входе** регистра RG1 обозначим **$P(1)$** , а вероятность нулевого – **$P(0) = P(1) + \Delta$** .

- Схема **выравнивания** вероятностей «Дельта-квадрат»



Все комбинации битов на выходе промежуточного регистра **RG1** и вероятности этих комбинаций (с учетом полной **статистической независимости** генерируемых соседних случайных битов) приведены в таблице:

Q1	Q2	Вероятности
0	0	$[P(1) + \Delta] * [P(1) + \Delta]$
0	1	$[P(1) + \Delta] * P(1)$
1	0	$P(1) * [P(1) + \Delta]$
1	1	$P(1) * P(1)$

- На выходе схемы **«ИСКЛЮЧАЮЩЕЕ ИЛИ»** формируется **логический нуль** при комбинациях, соответствующих **первой и последней** строкам таблицы:

$$P(0)' = [P(1) + \Delta] * [P(1) + \Delta] + P(1) * P(1).$$

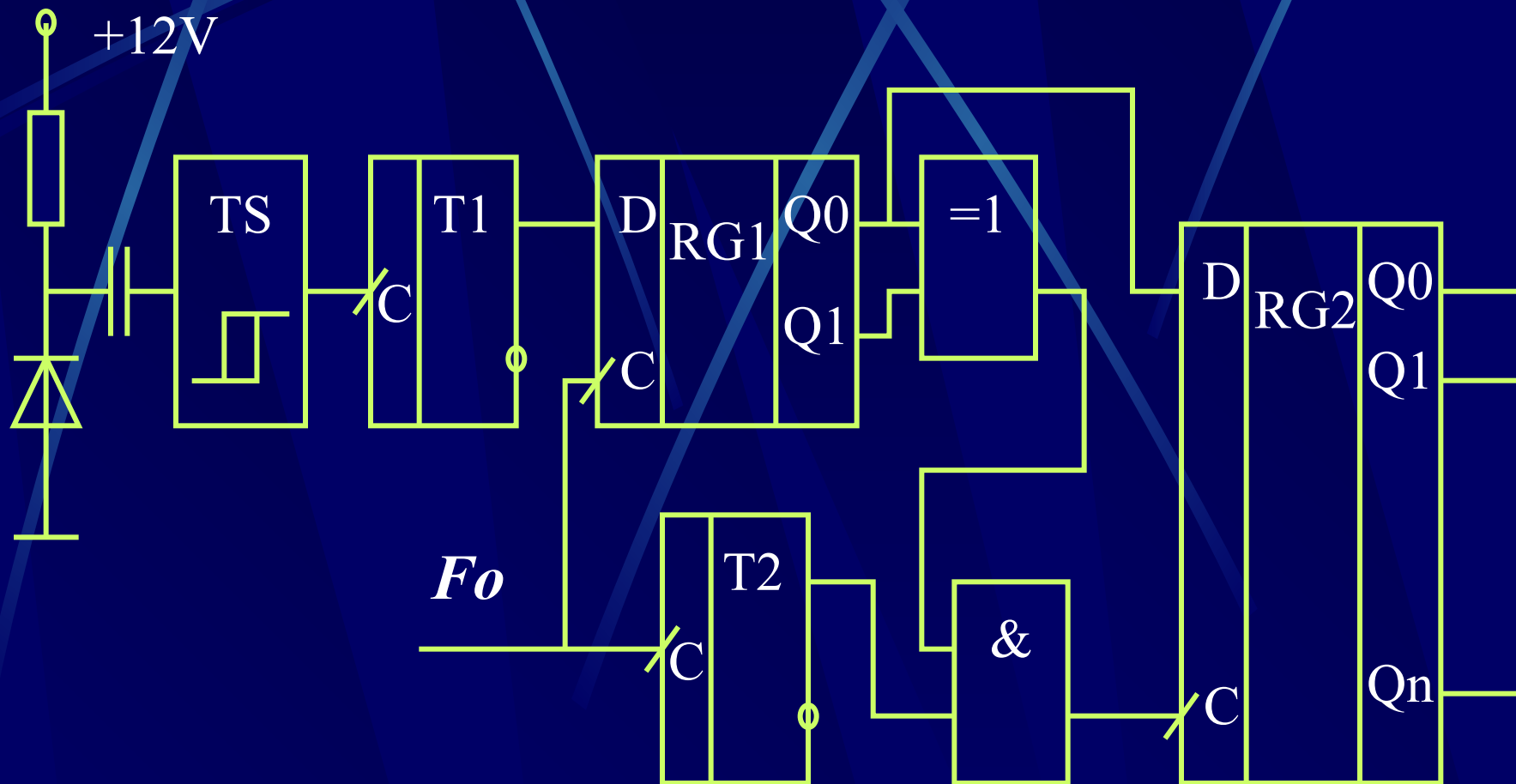
- Логической единице на выходе схемы **«ИСКЛЮЧАЮЩЕЕ ИЛИ»** будут соответствовать **две средние строки** в таблице:

$$P(1)' = [P(1) + \Delta] * P(1) + P(1) * [P(1) + \Delta].$$

- **Разность вероятностей** на выходе схемы **«ИСКЛЮЧАЮЩЕЕ ИЛИ»** Δ' равна:

$$\Delta' = P(0)' - P(1)' = \Delta^2.$$

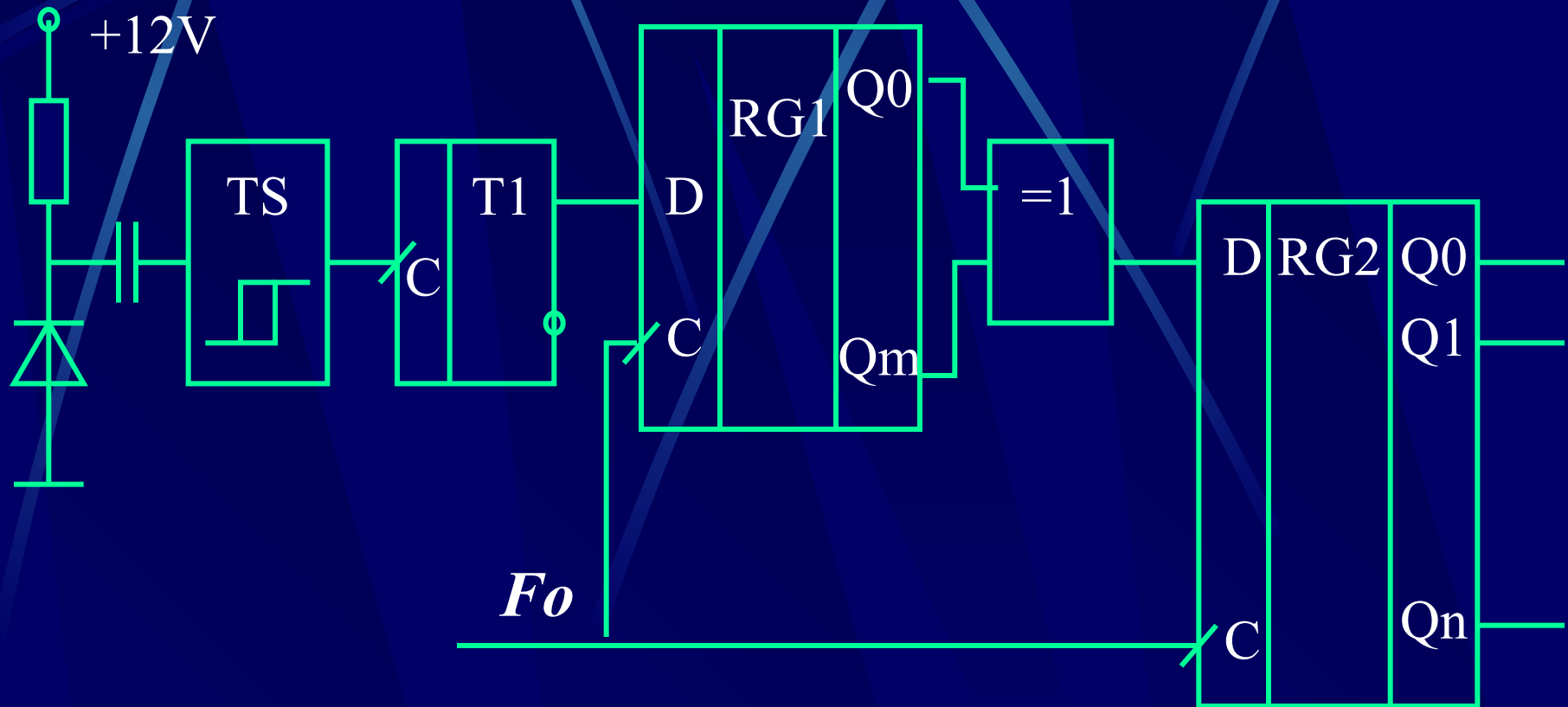
- Схема **ПОЛНОГО ВЫРАВНИВАНИЯ** вероятностей



МЕТОДЫ ПОВЫШЕНИЯ БЫСТРОДЕЙСТВИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

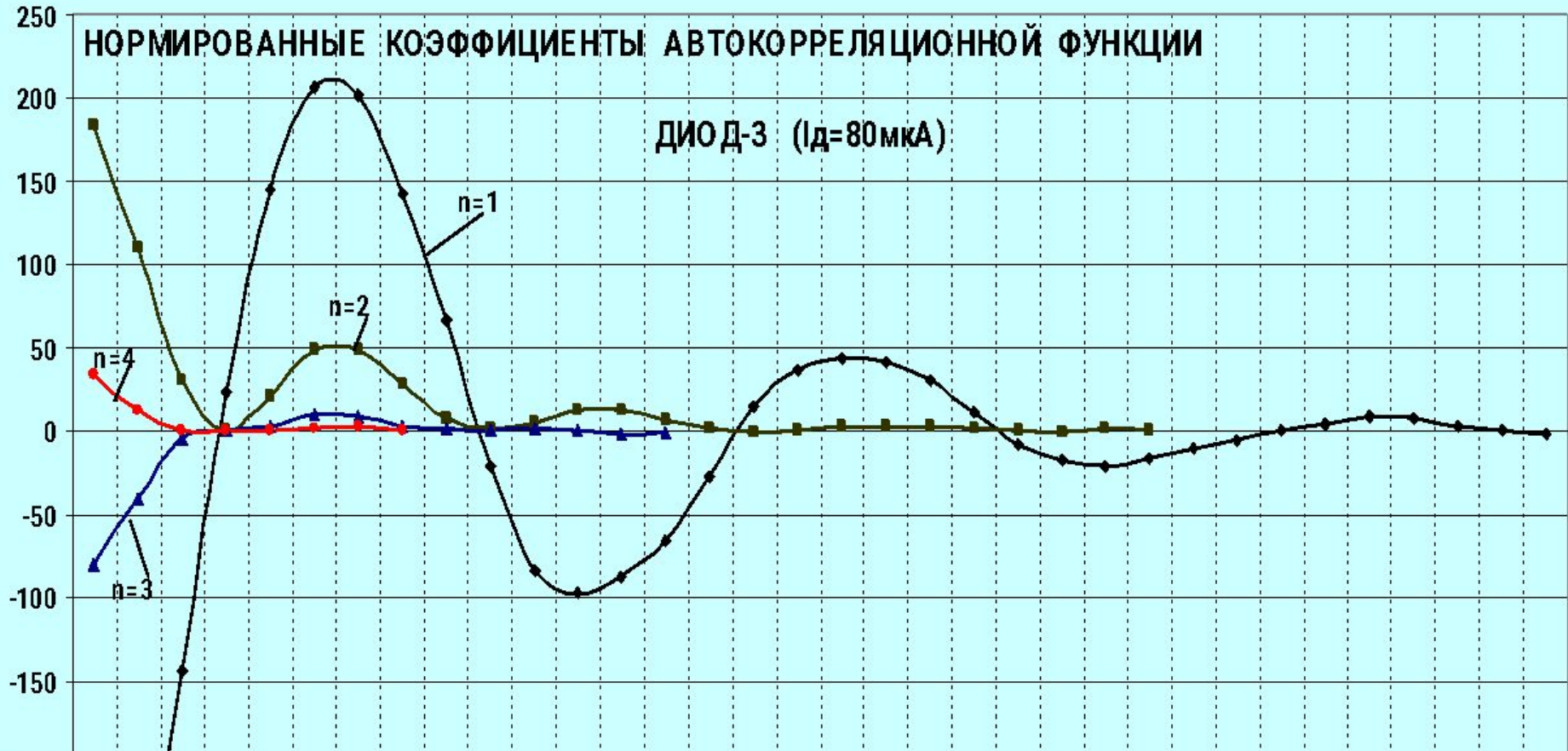
- Экспериментально было установлено, что применение схемы выравнивания вероятностей «Дельта-квадрат» с ростом скорости формирования случайных битов не только **не выравнивает вероятности** генерируемых случайных битов, а наоборот — **увеличивает разность вероятностей** по сравнению с исходными значениями (без применения схем выравнивания).

- Объединение двух или более независимых случайных процессов логическим элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ».



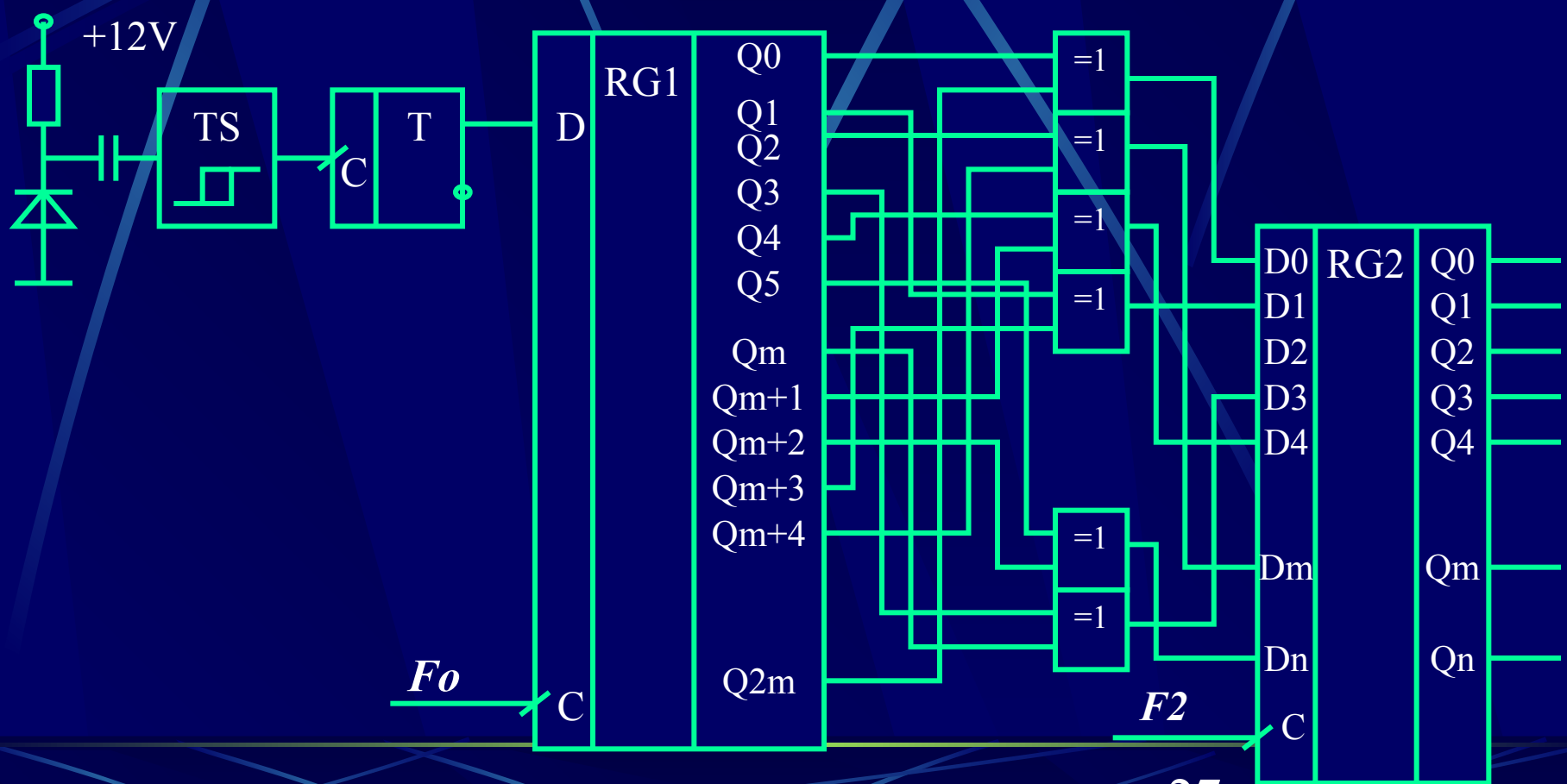
НОРМИРОВАННЫЕ КОЭФФИЦИЕНТЫ АВТОКОРРЕЛЯЦИОННОЙ ФУНКЦИИ

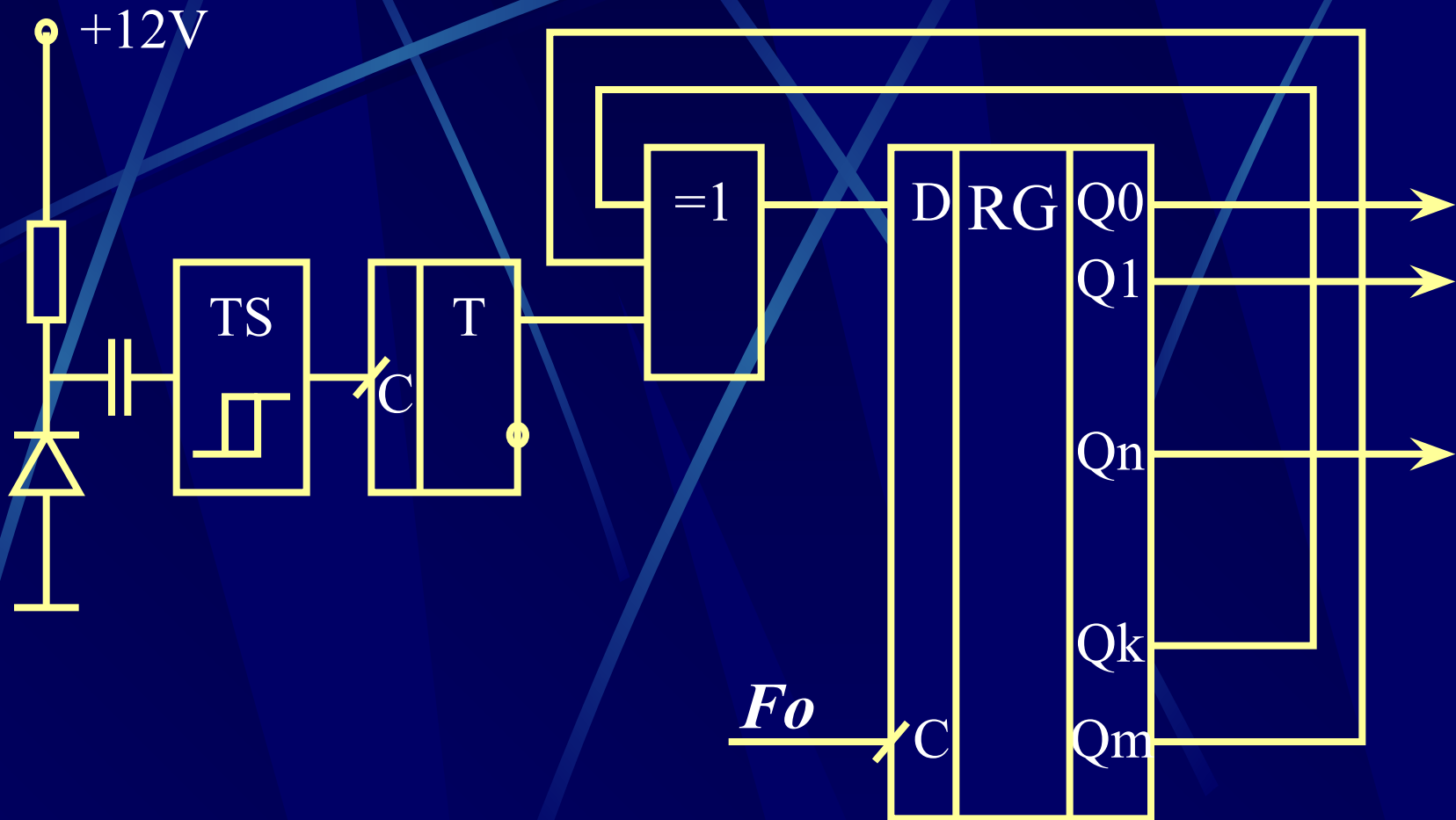
ДИОД Д-3 ($I_D=80\text{мкА}$)



Fш/Фо	1,0	1,2	1,4	1,5	1,7	1,9	2,1	2,2	2,4	2,6	2,7	2,9	3,1	3,3	3,4	3,6	3,8	4,0	4,1	4,3	4,5	4,6	4,8	5,0	5,2	5,3	5,5	5,7	5,8	6,0	6,2	6,4	6,5	6,7	
n=1	-404	-307	-145	22,8	145	206	202	143	66,7	-21	-85	-97	-88	-66	-27	14,3	37	43,2	41,1	30,6	10,9	-8,4	-18	-22	-16	-11	-5,9	0,56	3,4	9	7	3	0,8	-1,7	
n=2	184	110	30,1	-0,1	21,1	48,1	48,3	28,2	7,7	1,5	5,5	12,9	12,6	6,8	1,9	-1,2	0,1	3	2,9	2,8	1,4	0,02	-0,6	1,4	0,7										
n=3	-81	-41	-4,7	0,4	2,9	9,8	8,4	3	1,2	0,2	1,1	-0,3	-1,9	-0,4																					
n=4	33,7	12,3	0,5	0,8	-0,2	1,5	3	0,7																											

- Записывать в **параллельный регистр RG2** результат выполнения операций **«ИСКЛЮЧАЮЩЕЕ ИЛИ»** над сигналами с **первой** и **второй** половины **сдвигающего регистра RG1** с **перестановкой** **ВЫХОДНЫХ СИГНАЛОВ**

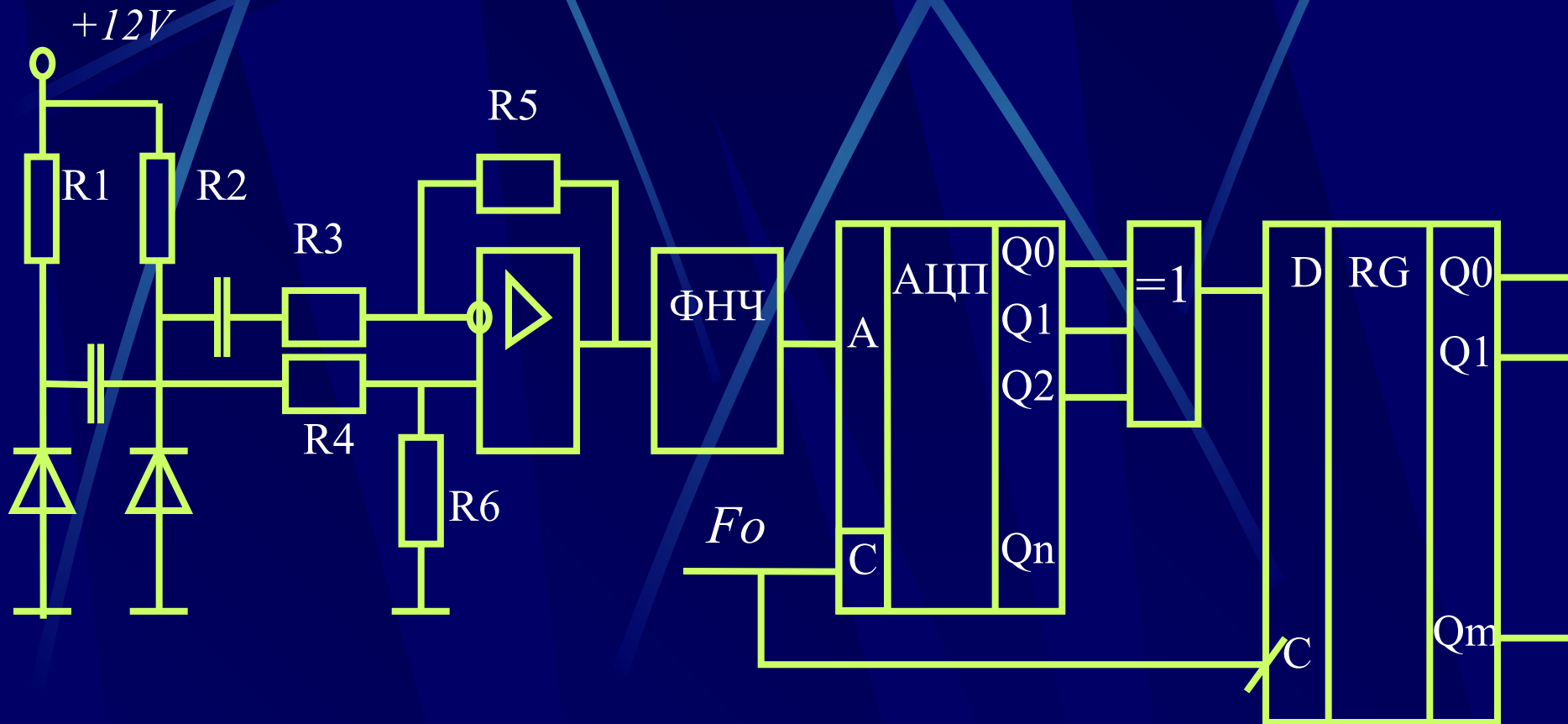




*Генератор случайных последовательностей
на основе ЛРР*

- Схему можно рассматривать как сдвигающий регистр, в который **вводятся случайные биты** от источника с **физическим датчиком шума**, а цепь обратной связи с элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» используется для улучшения статистических свойств случайной последовательности по методу **«Дельта-квадрат»**.
- Эту же схему можно рассматривать как генератор **псевдослучайных последовательностей** на основе ЛРР, в котором в случайные моменты времени **«разрушается рекуррента»** за счет **инверсии сигнала** обратной связи элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ», что делает такие последовательности **непредсказуемыми**, то есть случайными.

Генератор случайных последовательностей на основе АЦП



МЕТОДЫ ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ МЕТОДИКИ FIPS 140-1.

- Генераторы случайных битовых последовательностей, реализованные на **физических** источниках случайности, подвергнуты влиянию **внешних факторов**, а также **сбоям**.
- Поэтому такие устройства периодически необходимо **тестировать**, например, с помощью **статистических тестов**.

В американском федеральном стандарте **FIPS 140-1** используются четыре статистических теста на случайность:

- **МОНОБИТНЫЙ ТЕСТ,**
- **БЛОЧНЫЙ ТЕСТ,**
- **ТЕСТ СЕРИЙ И**
- **ТЕСТ ДЛИН СЕРИЙ.**

В этих тестах для удовлетворительных значений статистических параметров задаются **границы.**

Если какой-нибудь из тестов **не пройден**, то считается, что генератор (или последовательность) **не прошел тестирование.**

- Алгоритм тестирования **FIPS 140-1** может быть реализован **на программном уровне после ввода** последовательности s – 20000 случайных бит в **ПЭВМ**.
- Но в некоторых случаях тестирование случайных последовательностей необходимо производить **в аппаратном модуле** генерации случайных чисел (ГСЧ) **до ввода в ПЭВМ**.
- Для этих целей обычно применяют **одно-**
кристальные микро-ЭВМ (ОМЭВМ) –
микроконтроллеры (МК).

- Для того, чтобы **достоверно** измерить разность вероятностей $P(1)-P(0)=10^{-12}$, необходимо сгенерировать случайную битовую последовательность длиной не менее **10^{24} бита.**
- При частоте генерации случайных битовых последовательностей **16 Мбит/с** для этого понадобится более **1 000 000 000 лет.**

ΔP	10^{-5}	10^{-6}	10^{-7}	10^{-8}
N, бит	10^{10}	10^{12}	10^{14}	10^{16}
Время	20 мин.	30 час.	4 мес.	30 лет

Вопросы для экспресс-контроля

- Назовите основные отличия случайных последовательностей от псевдослучайных.
- Назовите методы генерации псевдослучайных последовательностей.
- Назовите основные источники физического шума для генерации случайных последовательностей.
- Перечислите основные тесты американского стандарта тестирования случайных последовательностей **FIPS 140-1**.
- Назовите методы выравнивания вероятностей случайных битовых последовательностей.

Лекция окончена

- Спасибо за внимание