Generátor náhodných čísel založený na radioaktivním rozpadu

Jan Podloučka, Karel Klojda, Dennis Ryšánek

Problematika generování náhodných čísel

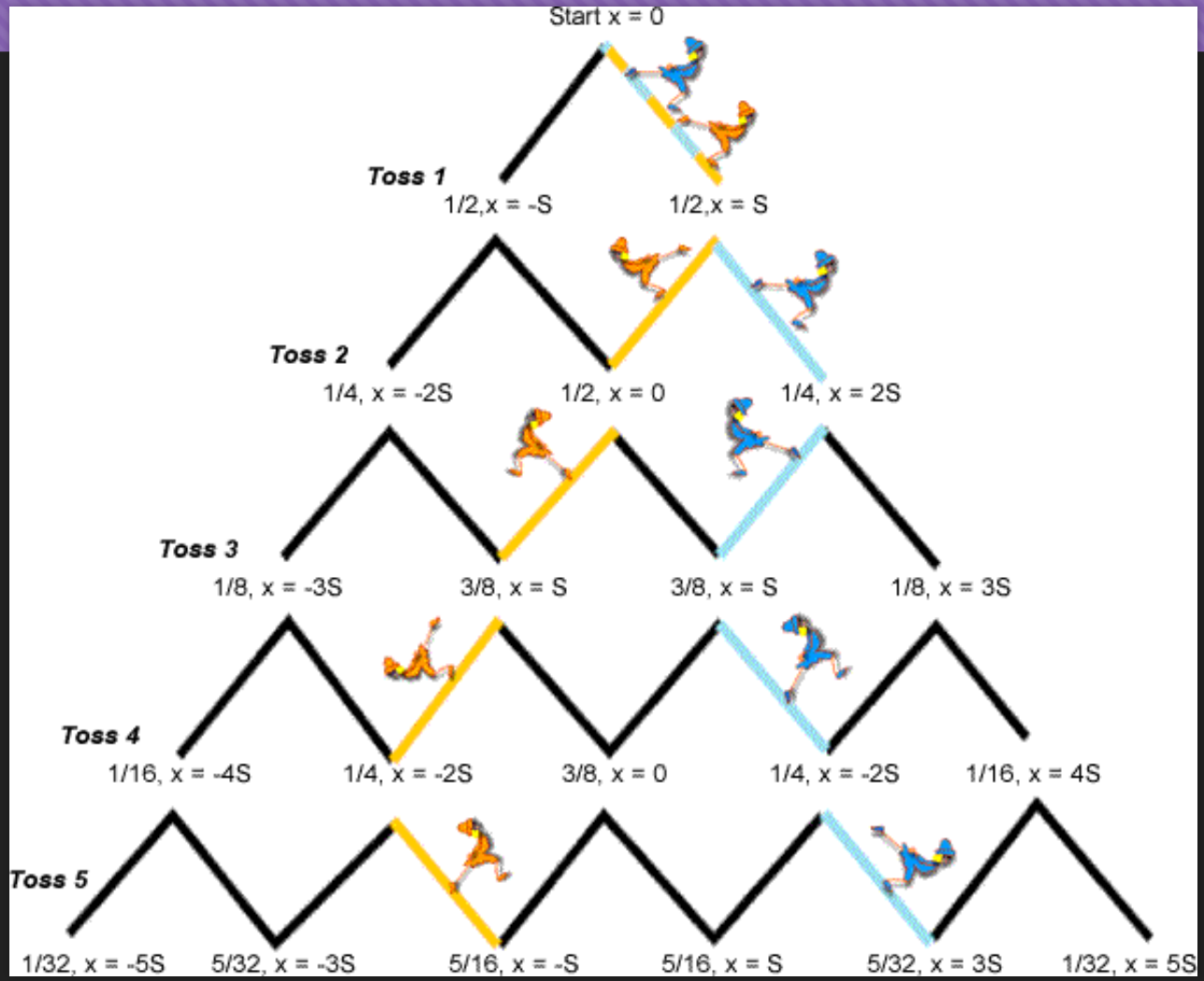
- Hazardní hry (online kasina…)
- Počítačové simulace (např. Monte Carlo)
- Šifrování

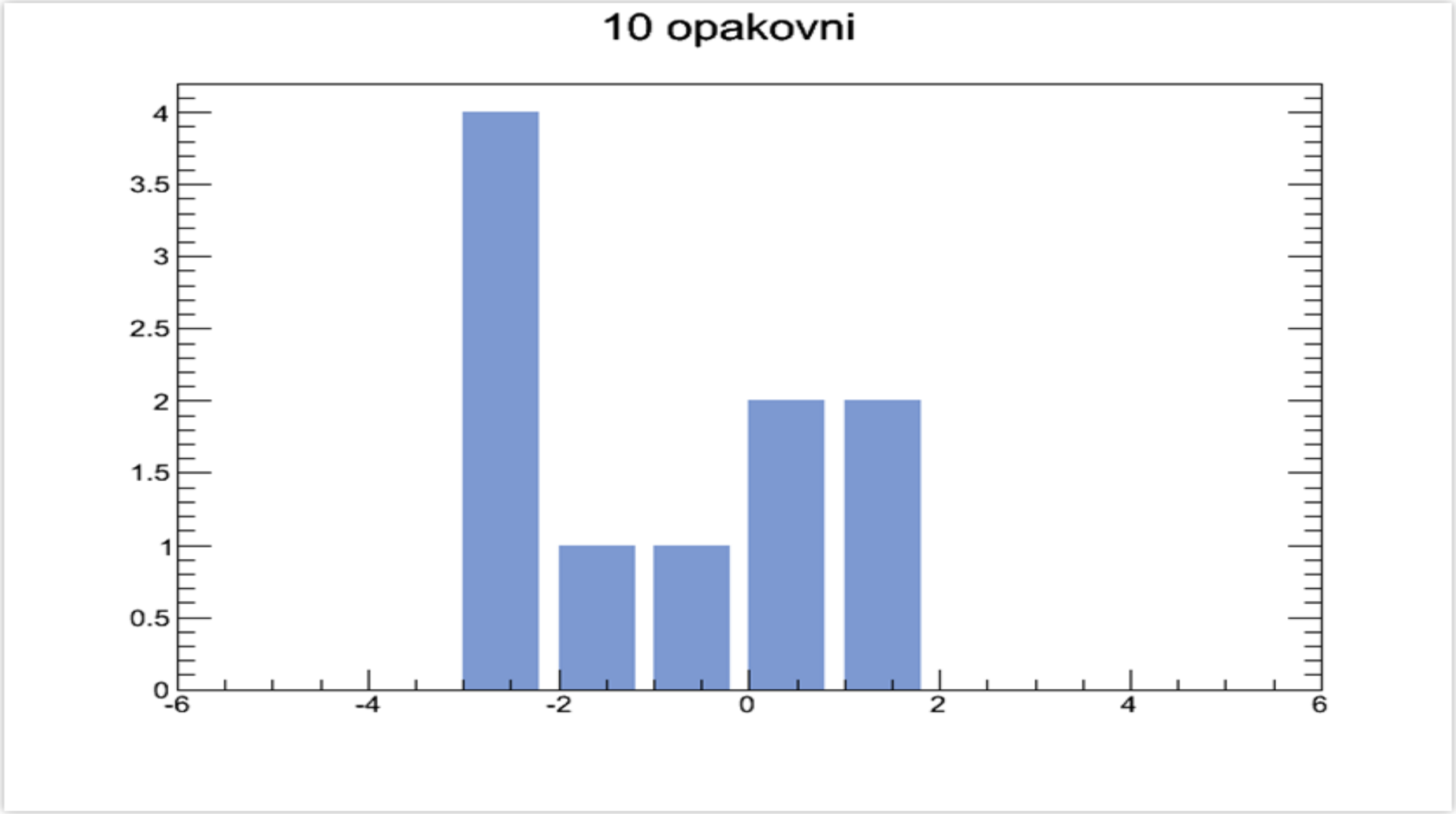
Možnosti generování

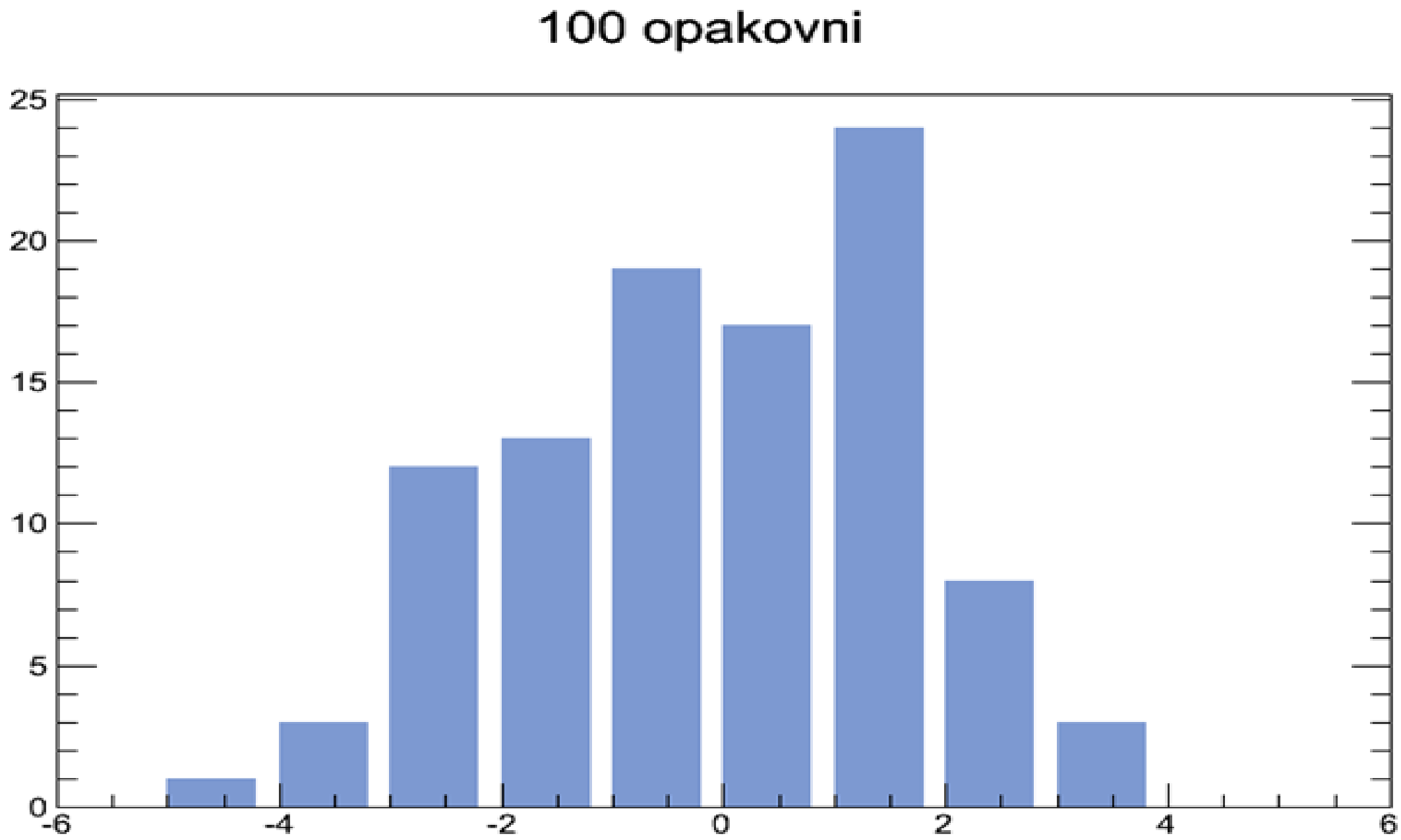
- Pseudonáhodné
  - Matematické posloupnosti
  - Složité i jednoduché algoritmy
- Náhodné – náhodné fyzikální procesy
  - Radioaktivní rozpad
  - Hod mincí/kostkou
  - Random.org (založena na atmosférických jevech)

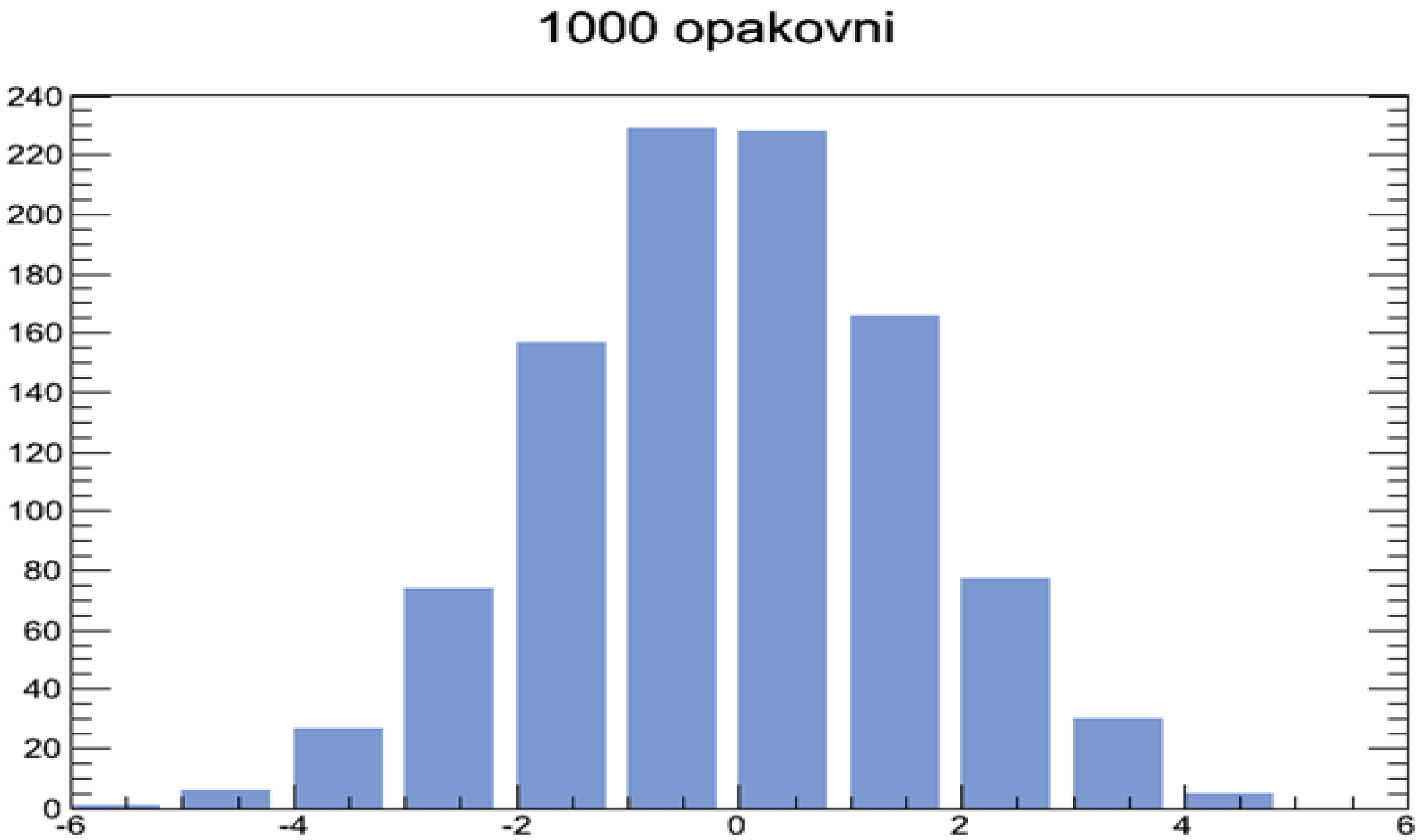
Metoda Monte Carlo

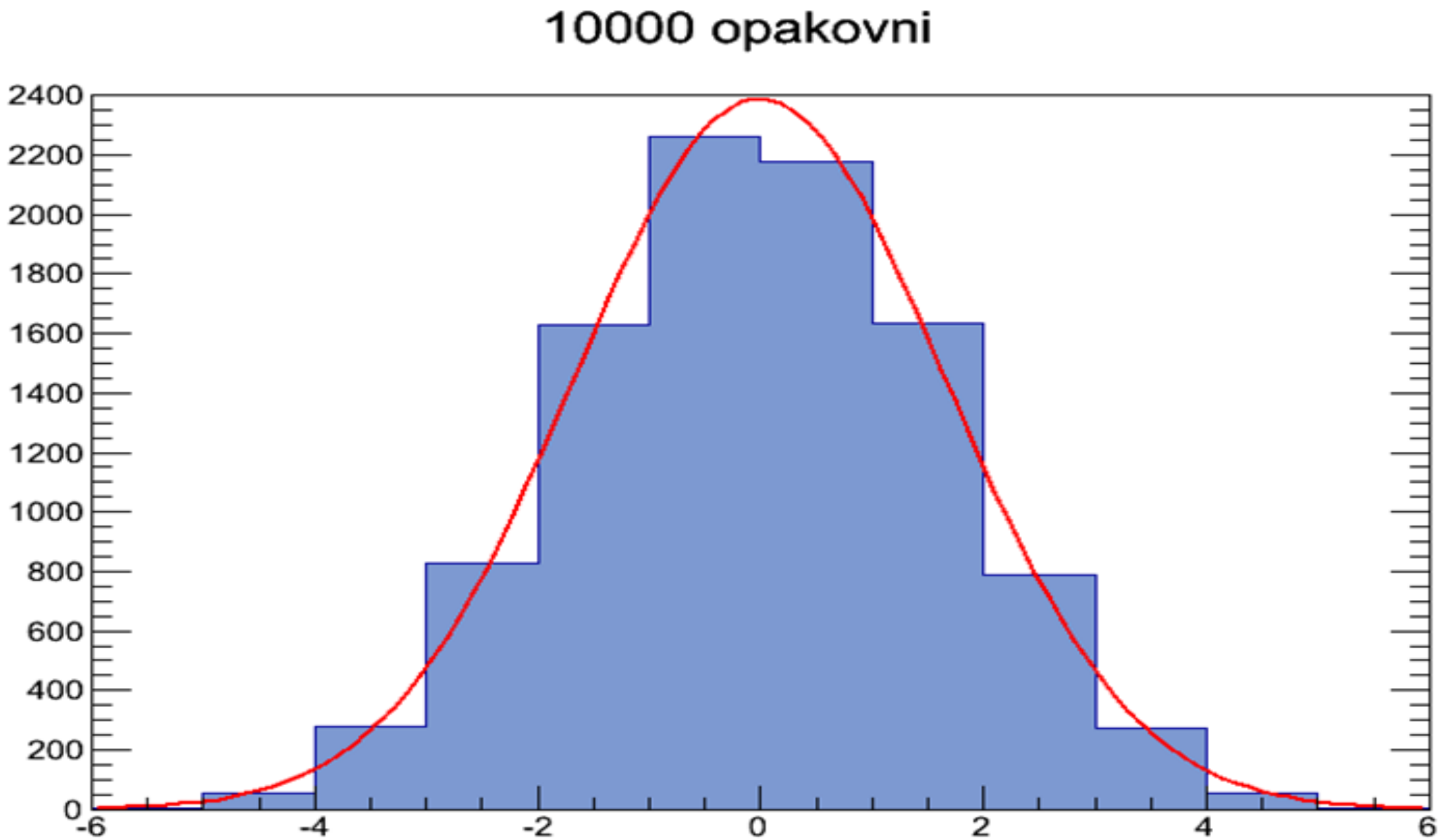
Simulace náhodné procházky




10 opakovni
4
3.5
3
2.5
2
1.5
1
0.5
0
-6
-4
-2
0
2
4
6

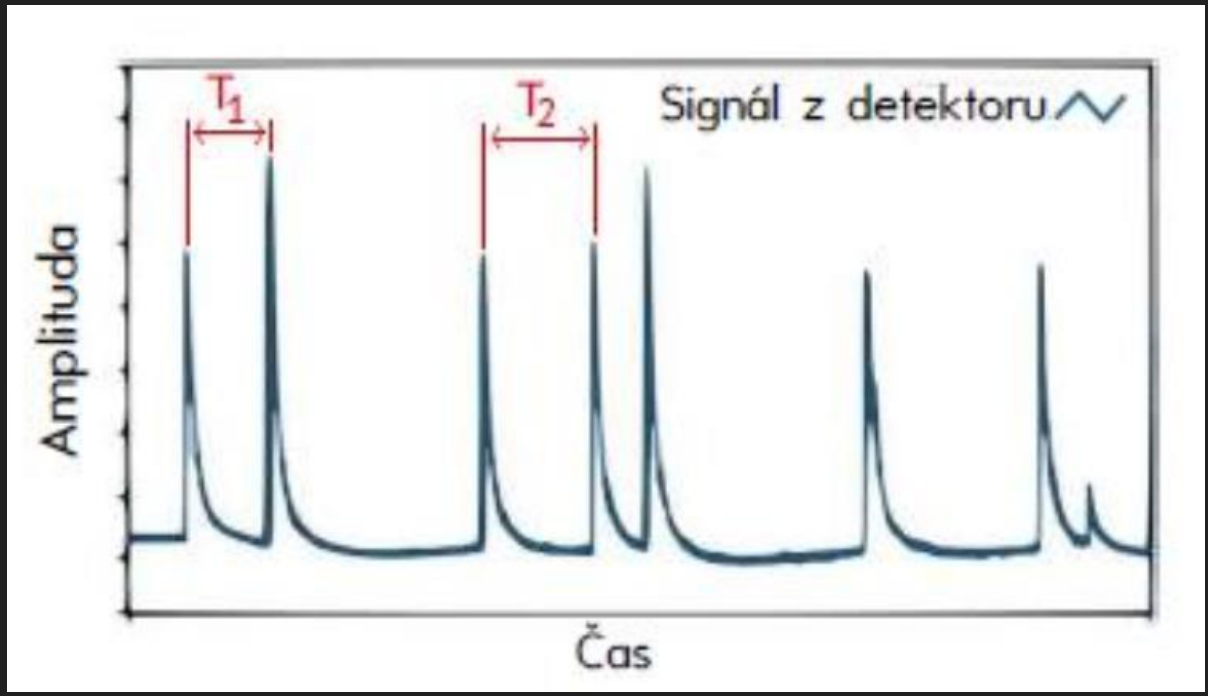

100 opakovni
25
20
15
10
5
0
-6
-4
-2
0
2
4
6


1000 opakovni
240
220
200
180
160
140
120
100
80
60
40
20
0
-6
-4
-2
0
2
4
6

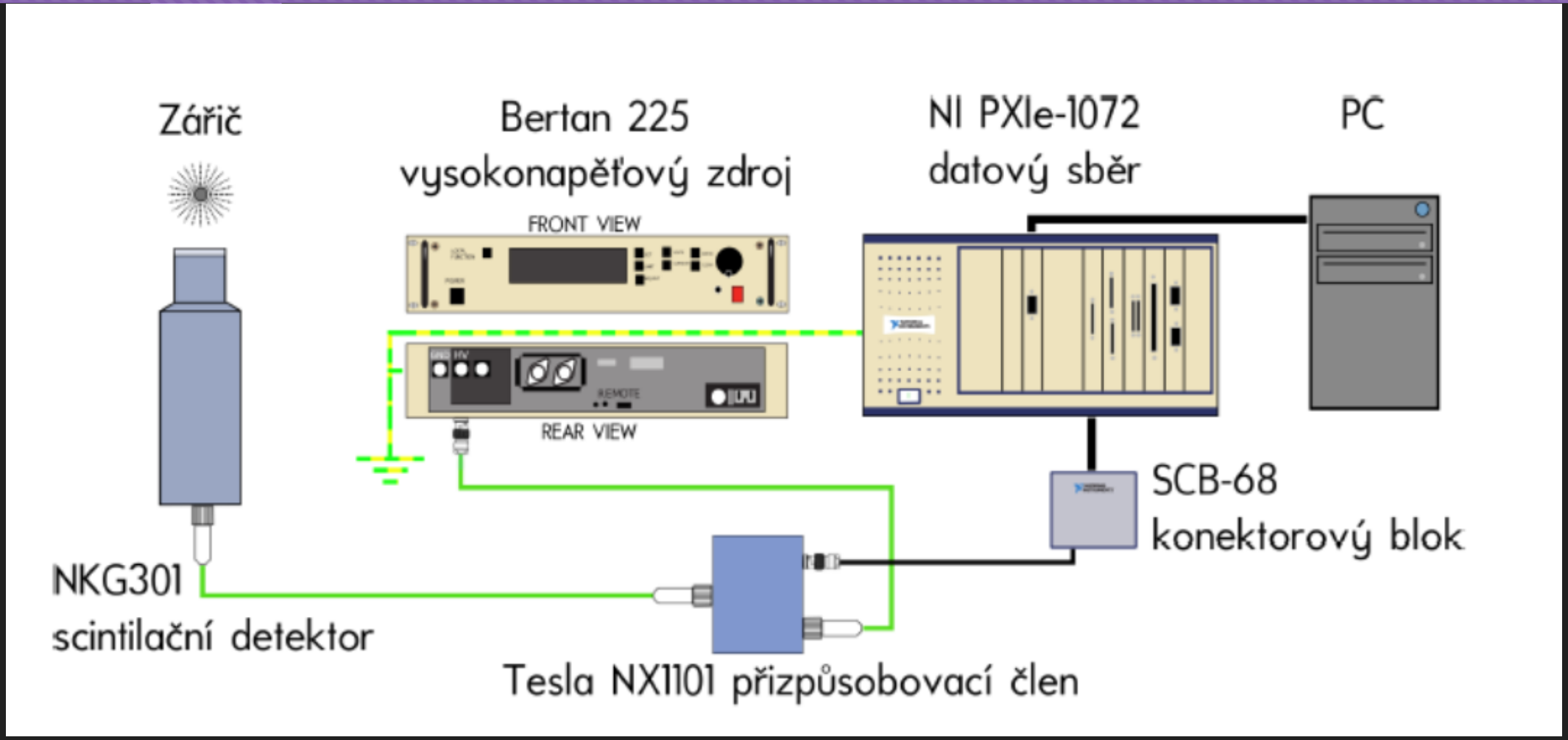

10000 opakovni
2400
2200
2000
1800
1600
1400
1200
1000
800
600
400
200
0
-6
-4
-2
0
2
4
6

Princip generování na radioaktivním rozpadu

- Měření rozdílů časů mezi vrcholy
  - $T_1 > T_2 \rightarrow 0$
  - $T_2 > T_1 \rightarrow 1$
  - $T_1 = T_2 \rightarrow$ vypouští se
- John von Neumannův dekorelátor
  - 00 nebo 11 → vypouští se
  - 01 → 0
  - 10 → 1

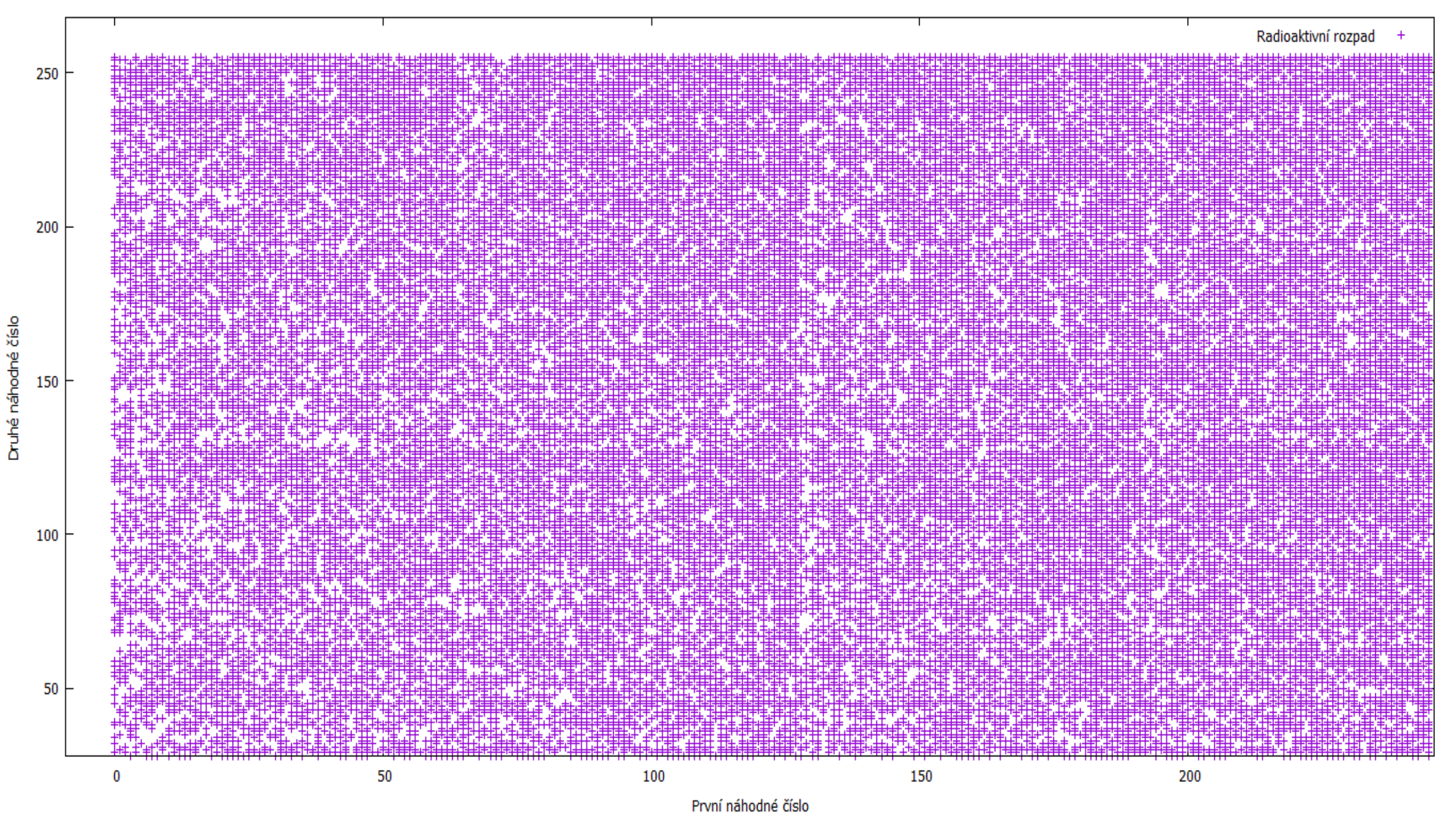


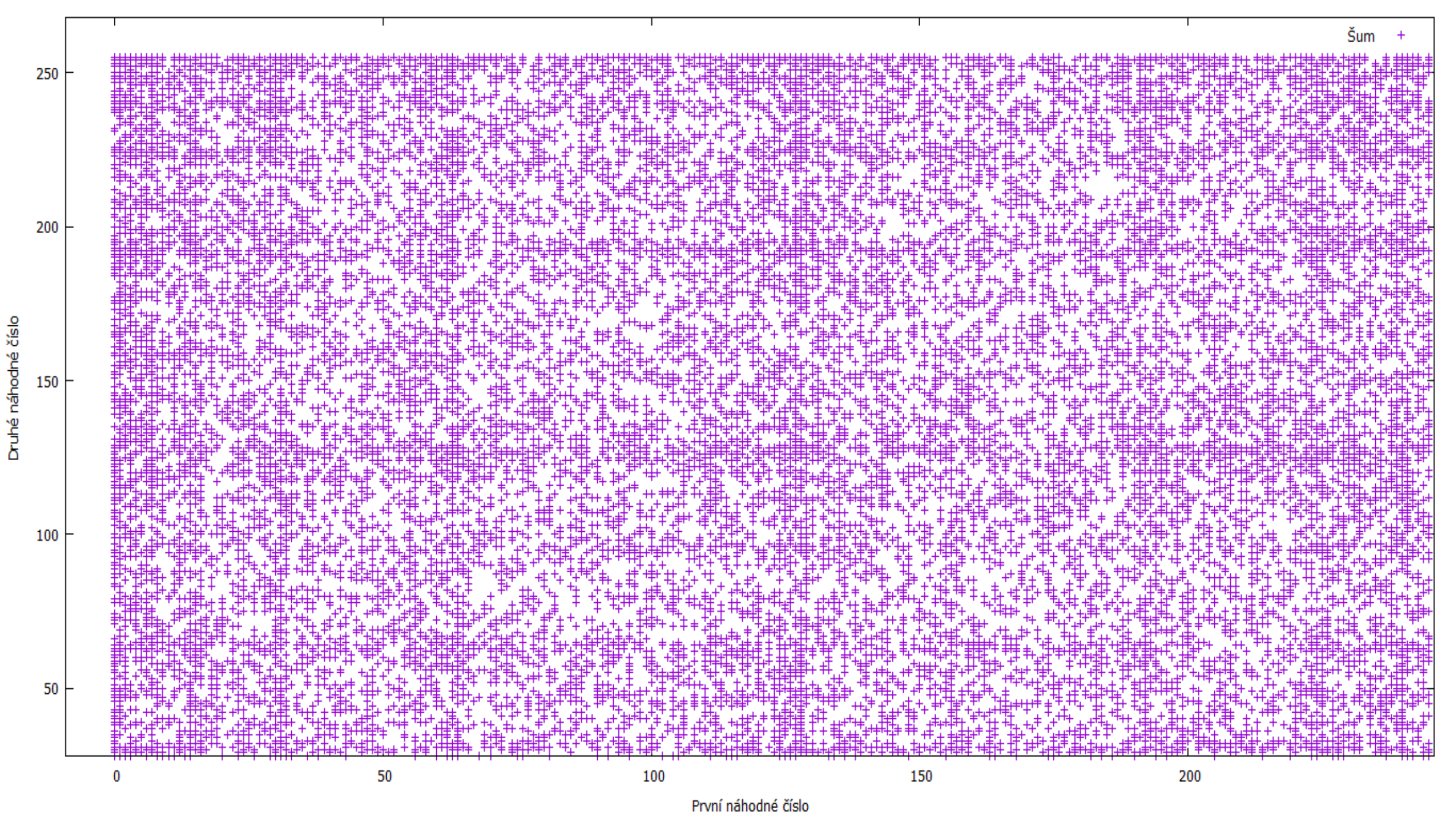
Aparatura

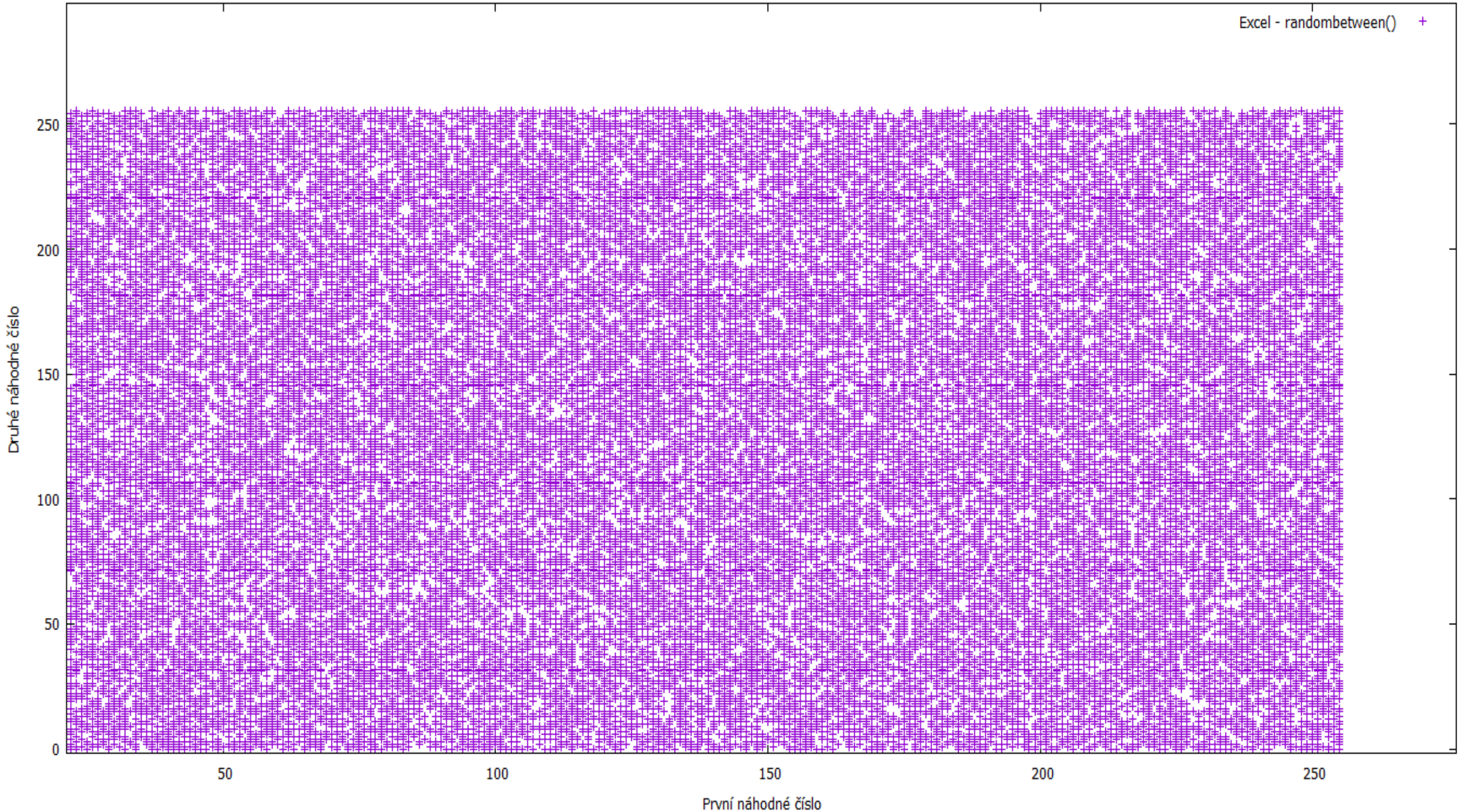

Zářič
Bertan 225
vysokonapěťový zdroj
FRONT VIEW
REAR VIEW
NI PXIe-1072
datový sběr
PC
SCB-68
konektorový blok
NKG301
scintilační detektor
Tesla NX1101 přizpůsobovací člen

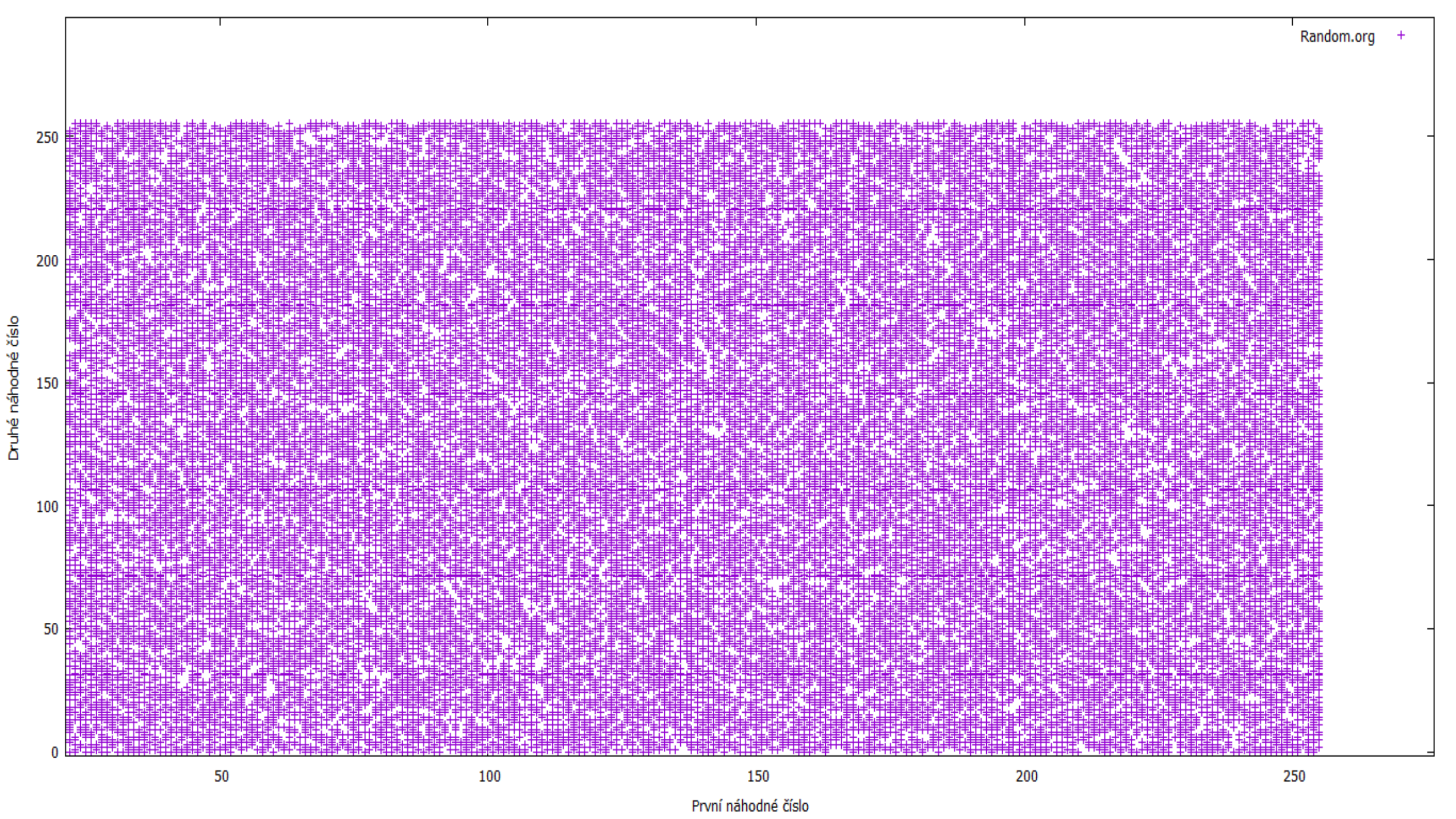
Výsledky

- Radioaktivní rozpad
- Šum
- Excel – randbetween()
- Random.org


Radioaktivní rozpad
250
200
150
100
50
Druhé náhodné číslo
0
50
100
150
200
První náhodné číslo


Šum
250
200
150
100
50
0
50
100
150
200
Druhé náhodné číslo
První náhodné číslo


Excel - randombetween()
Druhé náhodné číslo
První náhodné číslo
0
50
100
150
200
250


Random.org
Druhé náhodné číslo
První náhodné číslo
0
50
100
150
200
250

Zhodnocení výsledků

- Nepodařilo se vygenerovat náhodná čísla
- Excel – pseudonáhodný generátor - lepší výsledky
- Random.org – zjistili jsme nenáhodnost