

Опис програмного забезпечення для будування ШНП

Для формування шаблону нормальної поведінки застосунок збирає інформацію з картинки – графіку статистики значень параметрів безпеки.

Програмно визначаються:

- Кількість рівнів, у яких перебувають значення в кожний момент часу, останній приймається за заборонений.
- Крок часу.

Реалізація ланцюгів Маркова виконується за допомогою рівнянь Колмогорова-Чепмена:

$$\frac{dP_0(t)}{dt} = -\lambda_0 P_0(t),$$

$$\frac{dP_1(t)}{dt} = P_0(t)\lambda_0 - P_1(t)\lambda_1,$$

...

$$\frac{dP_m(t)}{dt} = P_{m-1}(t)\lambda_{m-1} - P_m(t)\lambda_m,$$

$$\frac{dP_{m+1}(t)}{dt} = \lambda_m P_m(t).$$

Робота програми

Задання параметрів для аналізу статистики:

```
int levels = 11, step = 2, t1Param = 120;  
Bitmap image = new Bitmap(@"D:\Docs\KPI\Labs\CyberSecurity\Lab2\test1.png", true);
```

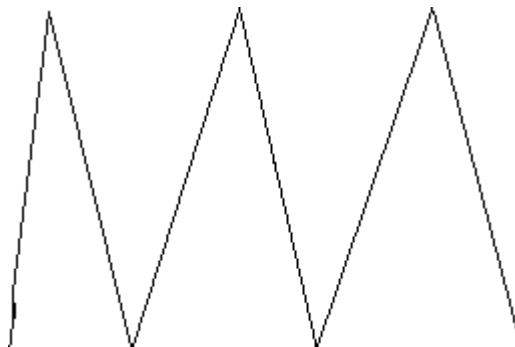


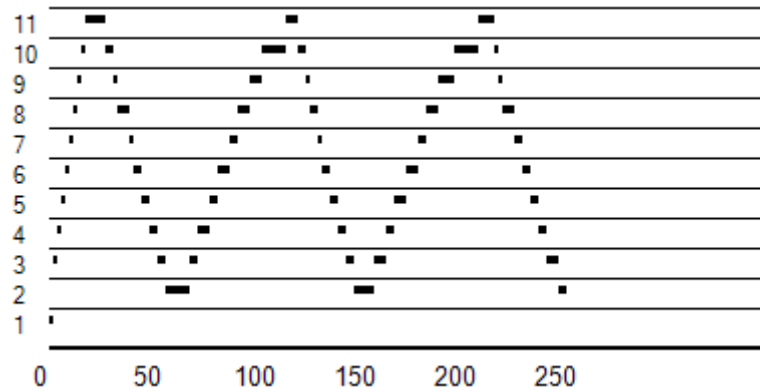
Рис. 1 – test1.png

Статистика збирається шляхом рахування переходів з одного рівня в інший окремо на кожному проміжку зростання і спадання. Для кожного такого проміжку формується список усіх ймовірностей переходів. З цих списків ймовірностей формується шаблон нормальної поведінки – графік

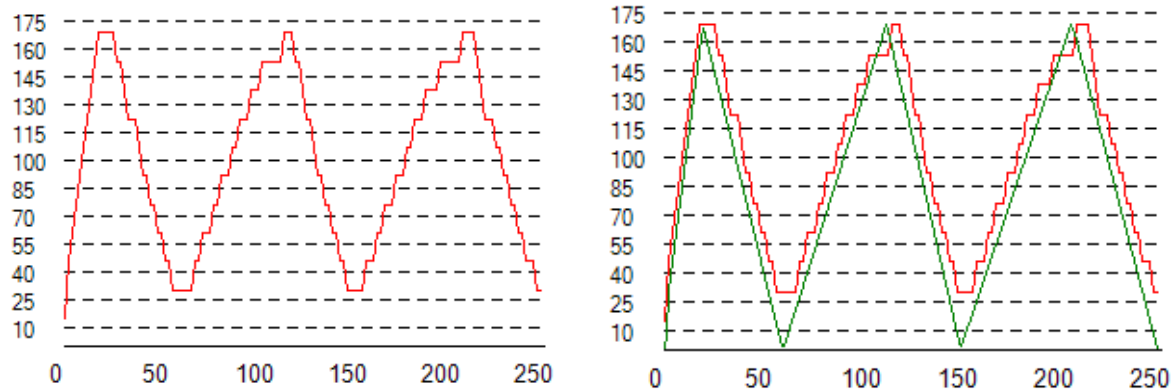
математичного очікування для кожного моменту часу і можливість побудування графіку відображення моделі поступової кібератаки.

Результати програми для графіку на рис.1 (11 рівнів, крок 2)

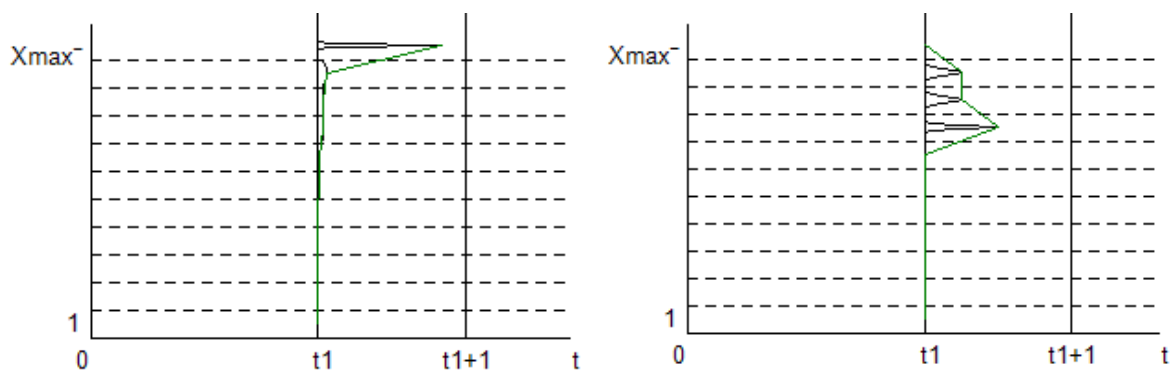
Графік відповідності значень ШНП до рівнів:



Графіки ШНП і порівняння ШНП з реальним графіком:

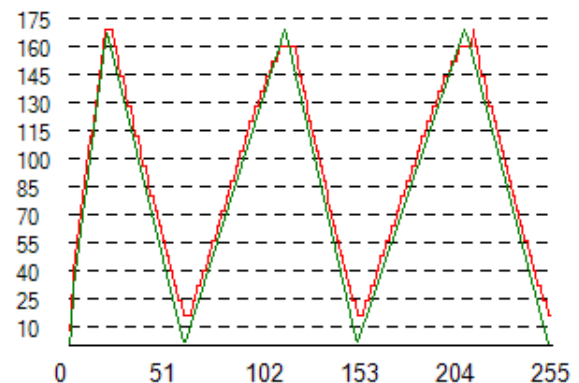
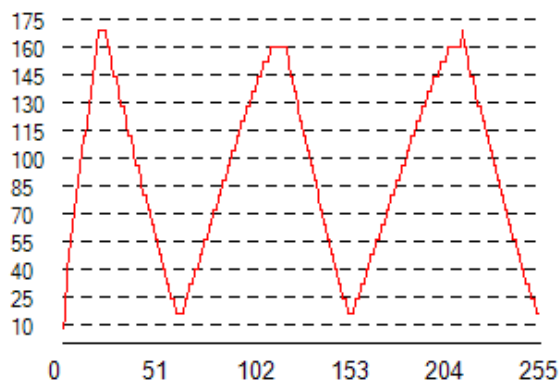
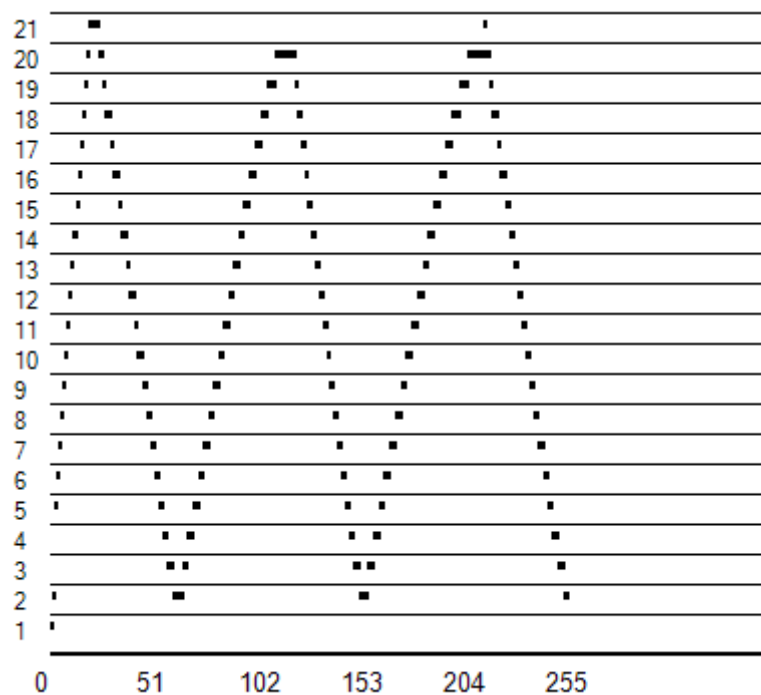


Графік відображення моделі поступової кібератаки в моменти $t_1 = 122, 130$:



Розглянемо роботу програми з найменшим можливим кроком (1) і більшою кількістю рівнів – 21.

Ті ж самі графіки для більш точних значень:



Як бачимо, загалом графік став більш схожий на реальний, але є суттєві неточності в крайніх точках. Це зумовлено ймовірностями переходів:

Перша крайня точка:

From 20 To 21, Probability = 1

Друга:

From 20 To 20, Probability = 0,666666666666667

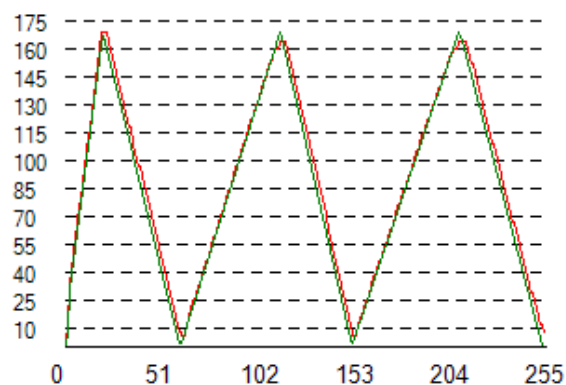
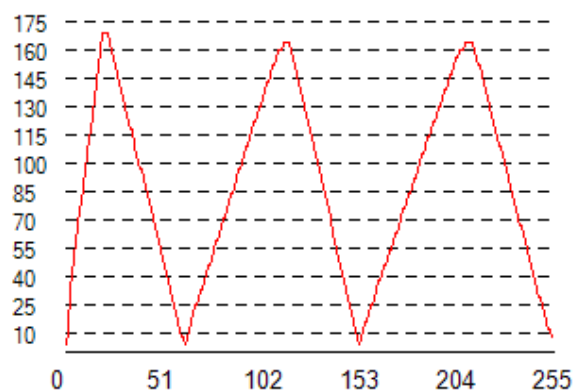
From 20 To 21, Probability = 0,333333333333333

Третя:

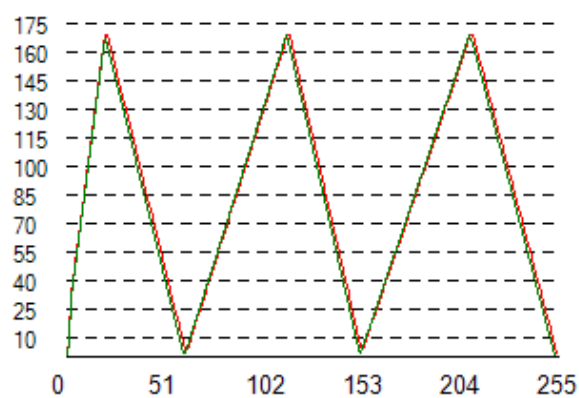
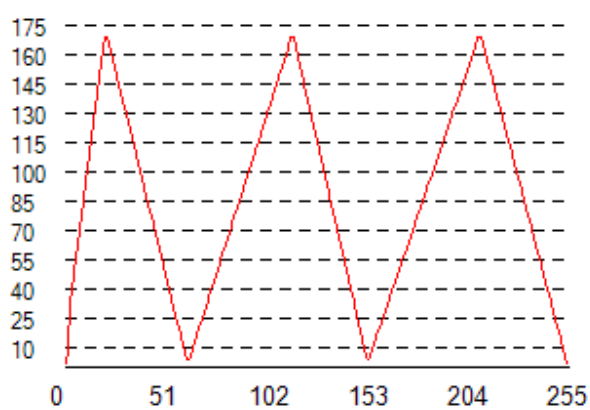
From 20 To 20, Probability = 0,5

From 20 To 21, Probability = 0,5

Графік ШНП і порівняння ШНП з реальним графіком для кількості рівнів 40:



Кількість рівнів 80:



Тобто із суттєвим збільшенням кількості рівнів ШНП, який базується на математичному сподіванні стане абсолютно ідентичним до реального графіку.