

Коефіцієнт a , який було знайдено раніше за МНК, береться із пам'яті контролера (див. рис. 4).

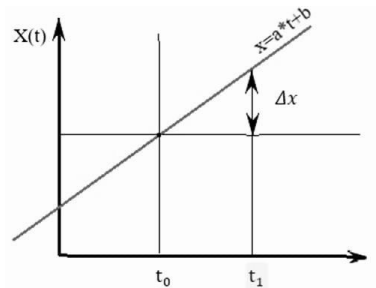


Рис. 4. Ілюстрація компенсації показників гіроскопа

ВИСНОВОК

В роботі запропоновано температурну компенсацію даних датчика MPU6050, які є залежними від температури. Побудовано експериментальний графік залежності показників гіроскопа від температури. За допомогою метода найменших квадратів отримано коефіцієнти лінійної апроксимації для лінійній області цієї залежності.

Список використаних джерел

1. Geier J. *Wireless Networks First-step*. 2004. 192 с.
2. УДК 004.73:685.648.683 Том 2 №13 (2021) *Безпроводна передача даних у тренажері «Боксерська груша»* Ю. В. Сіряк Д. В. Чернов 10.11.2021
3. Сіряк Ю. В. *Безпроводна передача даних у тренажері «Боксерська груша»*. 2021р.
4. *The Case of the Misguided Gyro*. 2017. URL: <https://www.analog.com/en/analog-dialogue/raqs/raq-issue-139.html>.
5. *Temperature compensation. It does matter*. 2021. URL: https://slugsuav.soe.ucsc.edu/flog/files/temperature_compensation.html.
6. Використання апроксимації методом найменших квадратів при експериментальному дослідженні механічних характеристик електроприводів А. О. Тригуб М. В. Пушкар. 2016. URL: <http://jour.fea.kpi.ua/article/view/102254>.

УДК 004.01

Соловійова А.К., здобувач
Ніколюк П.К., к.т.н., професор,
кафедри інформаційних технологій

МОДЕЛЮВАННЯ СТАТИСТИЧНИХ РОЗПОДІЛІВ ВИПАДКОВИХ ВЕЛИЧИН

Донецький національний університет імені Василя Стуса, м. Вінниця

В імітаційній моделі телекомунікаційної системи (ІМ ТКС) повинні бути відображені такі процеси [1]:

- надходження заявок;
- вибір обслуговуючого пристрою;
- обслуговування;
- звільнення.

ІМ ТКС включає засоби, що дозволяють імітувати:

- вхідний потік заявок;
- управління / розподілом заявок;
- обслуговування;
- вихідний потік заявок;
- статистичну обробку вхідних і вихідних параметрів.

Імітація вхідного потоку заявок

Потік заявок – це послідовність заявок (викликів), що надходять в систему обслуговування у визначені моменти часу: $t_1, t_2, t_3, \dots, t_i, \dots, t_c, \dots$, де t_i – це вимірюваний параметр, який може приймати визначені або довільні значення [2].

Детермінований потік – потік заявок у фіксовані моменти часу.

Стохастичний (випадковий) потік – потік заявок у випадкові моменти часу. Для визначення потоку заявок необхідно описати інтервал часу між сусідніми заявками:

$$\Delta t_k = t_k - t_{k-1}. \quad (1)$$

Для моделювання випадкового потоку заявок необхідно задати функцію розподілу $F(\Delta t)$ інтервалу часу між сусідніми заявками.

Найбільш часто для досліджень систем зв'язку використовується моделі найпростішого потоку. Для найпростішого потоку викликів розподіл числа викликів, що надходять за час t визначається за формулою Пуассона:

$$P_i(t) = \frac{(\lambda t)^i}{i!} e^{-\lambda t} \quad (2)$$

$P_i(t)$ – ймовірність надходження в точності i викликів найпростішого потоку за відрізок часу t .

Найпростіший потік також називають стаціонарним пуассонівським потоком [3].

Основні параметри найпростішого потоку:

- розподіл кількості заявок i за інтервал часу t
- розподіл інтервалу часу між сусідніми заявками в потоці
- математичне очікування і дисперсія числа заявок потоку і часу між сусідніми заявками в потоці.

Параметри найпростішого потоку:

- розподіл кількості заявок i за інтервал часу $t = 1$:

$$p_i(t = 1) = \frac{(\lambda)^i}{i!} e^{-\lambda} \quad (3)$$

- функція розподіл інтервалу часу Δt між сусідніми заявками в найпростішому потоці:

$$P(\Delta t) = P(\tau < \Delta t) = 1 - \lambda e^{-\lambda \Delta t} \quad (4)$$

По-суті, це ймовірність того, що за інтервал Δt надійде один і більше викликів.

- щільність розподілу ймовірності Δt :

$$p(\Delta t) = \lambda e^{-\lambda \Delta t} \quad (5)$$

Таким чином, розподіл проміжків часу між викликами найпростішого потоку підпорядковується показовому (негативного експоненціальним) законом [4].

Список використаних джерел

1. Алгоритмічні(імітаційні) моделі в економіці та підприємстві: <https://cutt.ly/0MwZDwK> (дата звернення 7.11.22)
2. Моделювання випадкових подій та величин: <https://cutt.ly/kMwZGjR> (дата звернення 7.11.22)
3. Імовірнісне моделювання. Моделювання випадкових процесів: <https://cutt.ly/uMwZX1Y> (дата звернення 7.11.22)
4. Випадкова величина: <https://cutt.ly/jMwZNpO> (дата звернення 7.11.22)

УДК 681.188:004.056.5

Станіславчук Д. О.,
здобувач 2 курсу спеціальності
125 «Кібербезпека»
Зелінська О.В., доцент кафедри
інформаційних технологій

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Донецький національний університет імені Василя Стуса, м. Вінниця

На сьогоднішній день одним з найцінніших ресурсів є інформація. З кожним днем її стає все більше, тому збільшується потреба в забезпеченні захисту. В забезпеченні інформаційної безпеки важливу роль відіграє криптографічний захист.

Криптографічний захист - вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо [1].

Ключовим поняттям тут є “Криптографія”.

Криптографія - наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації. Її розвиток пов'язаний з потребою передавати таємну інформацію [2].