5. Шемаєв В.М., Присяжнюк М.М., Онофрійчук А.П. Соціальні мережі в аспекті інформаційної безпеки. *Наука і оборона*. 2019, №3. С.36-39.

Одержано 25.04.2023

УДК 621.3.01+621.38

КЛІМУШИН Петро Сергійович,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1020-9399;

СОЛЯНИК Тетяна Миколаївна,
кандидат технічних наук, доцент,
провідний науковий співробітник науково-дослідної лабораторії
з проблем інформаційних технологій та
протидії злочинності у кіберпросторі
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-3695-0019;

САЛІБА Абдель Нур Ліван,
кафедра інформаційно-вимірювальних технологій і систем
Національного технічного університету
«Харківський політехнічний інститут»
https://orcid.org/0000-0002-6954-3754

ГЕНЕРАТОРИ ХАОТИЧНОЇ ПОВЕДІНКИ ДЛЯ ПІДТРИМКИ КРИПТОГРАФІЇ У ПРИСТРОЯХ ІНТЕРНЕТУ РЕЧЕЙ

Мережа інтернет речей (Internet of Things – IoT) - є найважливішим трендом розвитку інформаційних технологій, що сприяє суспільному розвитку в сфері сервісу життя людей, громадської безпеки, медичних послуг, управління виробничими процесами, транспорту, конкурентоспроможності та продуктивності бізнесу.

Взаємопов’язаність вузлів IoT, підключених до мережі, негативно впливає на загальний рівень криптостійкості системи. Ця проблема посилюється факторами масовості, неоднорідністю структури задіяних пристроїв, обмеженістю обчислювальних та енергетичних ресурсів, автоматичністю підключення вузлів IoT до мережі, довірливістю з боку користувачів та захисту їх персональних даних та приватного життя. Проблеми безпеки є основним стримуючим фактором використання IoT мереж.

Метою дослідження є визначення криптостійких методів та засобів генерування істинно випадкових послідовностей, придатних для використання в системах криптографічного захисту мережі пристроїв IoT з обмеженими обчислювальними та енергетичними ресурсами [1].

Первісною основою криптографічного захисту рішень IoT є істинна випадковість послідовностей чисел генераторів випадкових чисел (ГВЧ).

Генерування випадкових послідовностей програмним шляхом за детермінованим алгоритмом у високопродуктивних мікропроцесорних системах не забезпечує належну якість цих послідовностей. Такі послідовності мають псевдовипадковий

характер, а отже зростає можливість їх передбачуваності і як результат знижується криптостійкість систем.

Тому на сьогоднішній день розроблено апаратні ГВЧ на основі різних фізичних процесів, таких як електричні шуми струму в електричних елементах, радіоактивний розпад, турбулентність атмосфери, космічне випромінювання, фотоелектричний ефект, квантові явища.

Проблема генераторів, які використовують фізичні процеси, в тому, що їх аналоговий контур марнує енергію. Крім того, важко зберегти працездатність цієї аналогової схеми через вдосконалення технічного процесу з виробництва мікросхем та їх мініатюризації. Тому важливо мати повністю цифрову схему, яка дозволяє мікропроцесору генерувати багатий потік випадкових значень без цих проблем.

Проведене дослідження показало, що останні кілька років активно досліджуються так звані «автономні бульові мережі» (АБМ). В сучасній науці відомі схеми АБМ, які демонструють хаотичну поведінку. Хаос виникає в умовах, коли робота мережі визначається найдрібнішими відхиленнями в напрузі живлення, зсувах фронтів через теплові флуктуації, наведень та інших факторів, що дестабілізують мережу.

Загальна функціональна схема АБМ з найменшим рівнем складності виконується з трьох логічних елементів (рис. 1), в якої можливі два варіанта схемного виконання: на двох елементах XOR (рис. 2) або XNOR (рис. 3) і одного вихідного тривхідового елемента зі спеціальною функцією, яка має назву «рахунок одиниць - блок 3» [2].

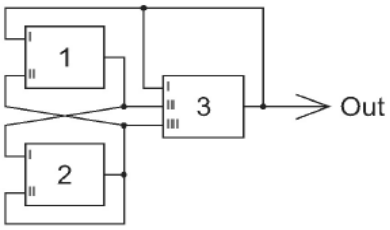

Рисунок 1 – Функціональна схема автономної бульової мережі

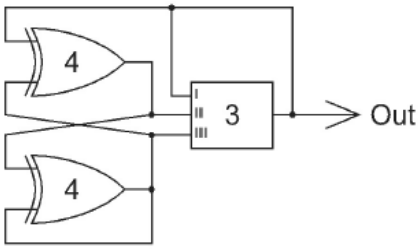

Рисунок 2 – Логічна схема автономної бульової мережі з використанням елементів XOR

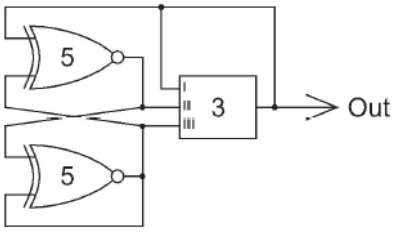

Рисунок 3 – Логічна схема автономної бульової мережі з використанням елементів XNOR

Такі однорозрядні блоки АБМ дозволяють створити ГВЧ з унікальними характеристиками: числа є дійсно випадковими; швидкість ГВЧ висока і обмежується затримкою розповсюдження сигналу через кілька логічних елементів (до 1.4 ГГц), а при реалізації на мікроконтролерах випадкове число можна отримати за один такт (до 3 ГГц); мінімальний розмір мережі робить її найекономічнішою з точки зору споживання енергії; генератор можна однаково ефективно реалізувати як на дискретних елементах, так і в інтегральному виконанні; конструкція генератора проста, мініатюрна та витрати на його реалізацію малі, що дозволяє використовувати його для підтримки криптографії у пристроях малоресурсних та енергозберігаючих пристроях IoT.

Таким чином, первинною основою криптостійкості рішень IoT є істинна випадковість послідовностей, які формуються ГВЧ і використовуються у алгоритмах криптографічного перетворення інформації для її захисту. Особливістю пристроїв

IoT є їх гетерогенність і територіальний розподіл, обмеженість обчислювальних ресурсів та електроживлення, мініатюрність.

Проведені дослідження показують, що найефективнішими для застосування в пристроях IoT є генератори хаотичної поведінки виключно на цифровій основі як автономні бульові мережі. Ці генератори мають потрібні для IoT характеристики: істинно випадкові числа, висока швидкість, мінімальне енергоспоживання, мініатюрність.

Перспективним напрямом розвитку АБМ є використання оптичних логічних вентилів для побудови оптичних АБМ з пропускною здатністю до 14 ГГц [3].

Список використаних джерел

1. Клімушин П. С., Соляник Т. М., Можаєв О. О., Гнусов Ю. В., Манжай О. В., Світличний В. А. Криптостійкі методи та генератори випадкових чисел у пристроях інтернет речей (IoT). Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20). С. 22–34. DOI: https://doi.org/10.30837/ITSSI.2022.20.022.

2. Goncharov S.V. Generator of truly random numbers. Description of the invention to patent RU2741865C1. 2021. 24c. URL: https://patents.google.com/patent/RU2741865C1/ru.

3. Optical Boolean chaos. Sang L., Zhang J., Zhao T., Virte M., Gong L., Wang Y. Optics Express. 2020. Vol. 28. No. 20. P. 29296–29305. URL: https://opg.optica.org/oe/fulltext.cfm?uri=oe-28-20-29296&id=439748.

Одержано 30.04.2023

УДК 004.81

КУРИЛО Дмитро Анатолійович,
курсант 1 курсу факультету 4
Харківського національного університету внутрішніх справ;

СВІТЛИЧНИЙ Віталій Анатолійович,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0003-3381-3350

ДЕЯКІ ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУСПІЛЬСТВІ

У сучасному світі штучний інтелект (ШІ) знаходить все більше застосувань у різних галузях науки та технологій. Ця технологія дозволяє комп'ютерам розуміти, аналізувати та використовувати великі обсяги даних для прийняття рішень. Застосування ШІ може значно покращити умови життя людей, забезпечити більш ефективне використання ресурсів та допомогти у боротьбі зі складними глобальними проблемами. Одним з найважливіших аспектів застосування ШІ є покращення умов життя людей. Штучний інтелект (ШІ) може допомогти суспільству у багатьох різних галузях і вирішувати складні проблеми, що стоять перед людством. Ось декілька прикладів того, як ШІ може покращити умови життя людей та сприяти розвитку суспільства [1]: