РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ГЕНЕРУВАННЯ НЕЛІНІЙНОЇ ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ

канд. техн. наук, проф. О.М. Рисований, студ. В.Р. Іванов, Національний технічний університет "Харківський політехнічний інститут", м. Харків

Нелінійна псевдовипадкова послідовність генерується з використанням нелінійних методів. Це методи, у яких вихід не є лінійною функцією від вхідних значень або станів генератора [1 – 3]. Тобто, у ланцюгу зворотного зв'язку використовується нелінійна передаточна функція.

В роботі наведено, що такі послідовності використовуються там, де лінійні генератори (наприклад, регістри зсуву з лінійним зворотним зв'язком – LFSR) не забезпечують достатню криптографічну стійкість, наприклад, у криптографії або моделюванні, де потрібно уникати передбачуваних шаблонів.

В роботі отримані всі перевірочні матриці в полі GF(3).

Зроблено висновок, що генерація максимальної послідовності поліномів – це процес створення всіх можливих поліномів обраного ступеня з заданими коефіцієнтами. Такий підхід має низку застосувань у математиці, інженерії, комп'ютерній науці та інших галузях.

Практична цінність отриманих в роботі результатів полягає в тому, що в рамках роботи розроблена програма генерування поліномів з максимальним періодом генерації станів та їх перевірочних матриць.

Список літератури: 1. Рисований О.М., Ігнатьєв К.І., Рибалка Р.В., Рудаковський Д.Р. Механізм шифрування повідомлень з максимальною довжиною // Інформатика, управління та штучний інтелект. Тези одинадцятої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – 176 с. – С.127. **2.** Рисований О.М., Ігнатьєв К.І., Рибалка Р.В., Рудаковський Д.Р. Вибір багаточленів з максимальним періодом генерації станів // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXXII міжнародної науково-практичної конференції MicroCAD-2024, 22-25 травня 2024 р. / за ред. проф. Сокола Є.І. – Харків: НТУ "ХПІ". – С. 1421. **3.** Рисований О.М. Криптостійкий генератор псевдовипадкової наслідності з використанням майстер-ключа // Проблеми інформатики та моделювання (ПІМ-2024). Тези двадцять четвертої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – С.120.