Міністерство освіти і науки України
Вінницький національний технічний університет

Матеріали LI науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2022)

31 травня 2022 року

Збірник доповідей

Електронне наукове видання

Вінниця
ВНТУ
2022

УДК 001
М34

Видається за рішенням Вченої ради Вінницького національного технічного університету Міністерства освіти і науки України

Головний редактор: В. В. Біліченко
Відповідальний за випуск: В. В. Грабко

Робоча група з підготовки конференції:
Голова робочої групи:
проректор з наукової роботи та міжнародного співробітництва ВНТУ В. В. Грабко;

Члени робочої групи:

декани факультетів, директор Інституту Конфуція ВНТУ;

Власюк А. І., начальник РВВ, доц.;

Могила С. Г., інженер 1-ї категорії РВВ;
Сідак С. Г., редактор РВВ;
Тамтура Я., О. редактор РВВ.

М34 **Матеріали** LI науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2022) : збірник доповідей [Електронний ресурс]. – Вінниця : ВНТУ, 2022. – (PDF, 2830 с.)
ISBN 987-966-641-894-7

Збірник містить тексти доповідей LI ювілейної регіональної науково-технічної конференції професорсько-викладацького складу, науковців, аспірантів та студентів Вінницького національного технічного університету з участю працівників підприємств м. Вінниці та Вінницької області з загально-інженерних, технічних, гуманітарних та фундаментальних наук.

НТКП ВНТУ проводиться у вигляді конференцій факультетів та конференції Інституту Конфуція ВНТУ. Кожна конференція має власну тематику, оргкомітет, строки проведення пленарних та секційних засідань, та складається з однієї або кількох секцій.

УДК 001

ISBN 978-966-641-894-7

Секція управління безпекою інформаційних систем та технологій

Секція суспільно-політичних наук

УДК 004.056.53

В. В. Сінюгін
В. С. Катаєв

РОЗРОБКА АПАРАТНОГО ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Вінницький національний технічний університет

Анотація

Було проведено аналіз проблеми захисту інформації при використанні генераторів шуму як засобів активного захисту. Розроблено апаратний генератор псевдовипадкових чисел, який може бути використаний у складі апаратних чи програмних генераторах шуму. Розроблений пристрій реалізовано на мікроконтролерній платформі Arduino, що дозволяє спростити як сам апаратний генератор псевдовипадкових чисел, так і генератори шуму. Реалізований алгоритм дає можливість отримати 2^{32} *псевдовипадкових чисел закономірність яких не прослідковується, а це в свою чергу дає можливість підвищити захищеність інформації шляхом ускладнення фільтрації корисних сигналів зловмисниками.*

Ключові слова: технічний захист інформації, генератор шуму, генератор псевдовипадкових чисел, Arduino, випадкові числа, системи захисту інформації.

Abstract

The analysis of the problem of information protection with using noise generators as a means of active protection was carried out. A hardware pseudo-random number generator has been developed that can be used as part of hardware or software noise generators. The developed device is implemented on the Arduino microcontroller platform, which simplifies both the hardware generator of pseudo-random numbers and the actual noise generators. The implemented algorithm makes it possible to obtain 2^{32} *pseudo-random numbers.*

Keywords: technical information protection, noise generator, pseudo-random number generator, Arduino, random numbers, information security systems.

Вступ

Актуальність даної роботи обумовлена постійно зростаючим впливом інформаційної компоненти як на подальший науково-технічний та соціально-економічний розвиток суспільства, так і на всі сфери життєдіяльності окремих особистостей. Інформація стає одним з головних чинників прогресу людської цивілізації і одночасно - суттєвим фактором загрози цьому розвитку, оскільки зростає небезпека можливості використання інформації з відверто антигуманними, злочинними намірами. Останнє загострює проблему несанкціонованого доступу до інформації. Виникає парадокс: глобальна інформатизація суспільства забезпечує нас новими прогресивними інформаційними технологіями, робить наше існування комфортнішим, цікавішим та інтенсивнішим, наповнюючи його засобами автоматизації, телекомунікації, зручною оргтехнікою, і водночас приводить до створення технічних засобів інформаційного впливу на особистість, до розробки найрізноманітніших засобів і методів технічної розвідки та інформаційного шпигунства [1]. Виходячи з цього, виникає потреба у вдосконалені засобів захисту інформації від витоку технічними каналами, що, в свою чергу, збільшить ефективність захисту інформації у виділених приміщеннях.

Для підвищення захищеності приміщення використовуються активні способи захисту інформації. Генератори шуму застосовуються для активного захисту інформації - постановки різноманітних перешкод [2]. Шум, що видається генератором, маскує корисний сигнал так, що виділити його серед загального сигналу стає дуже складним завданням. Якщо сигнал, що видається генератором, не є випадковим, на аналізаторі спектра можна побачити провали в спектральній характеристиці. Це є вразливістю в системах захисту інформації, побудованих за допомогою цих генераторів шуму, тому що є технічна можливість побудувати гребінчастий фільтр і виділити неспотворену частину корисного

сигналу, тобто якість захисту інформації від витоку залежить від алгоритму генерації шуму, тому що зловмисник може використовувати інструментарій, що фільтрує корисний сигнал від перешкод.

Принцип роботи генератора шуму (ГШ) полягає у створенні суміші сигналу і шуму. Вузькосмуговий фільтр (ВФ) виділяє певну смугу частот з цієї суміші і формує квазігармонійний процес, який надходить на модулятор. Далі цей сигнал модулюється псевдовипадковою послідовністю (ПВП) і через підсилювач (П) сформований генератором шумовий сигнал за допомогою активної акустичної системи чи антен випромінюється в простір або за допомогою вібродатчика вібрує на поверхню [3].

Тому ***метою*** даної роботи є розробка генератора псевдовипадкових чисел як складової частини генераторів шуму, який мав би у своєму складі сучасну елементну базу та міг бути запрограмований таким чином, щоб ускладнити процес фільтрації корисного сигналу зловмисниками.

Розробка апаратного генератора псевдовипадкових чисел

Генератор випадкових чисел (ГВЧ) являє собою пристрій, який генерує послідовність цифр або символів, які не можуть бути обґрунтовано прогнозованими краще, ніж за допомогою випадкового шансу. Генератори випадкових чисел можуть бути істинними апаратними генератори випадкових чисел (HRNG), які генерують дійсно випадкові числа, або псевдо-генератори випадкових чисел, які генерують числа, які виглядають випадковими, але насправді є детермінованими, і можуть бути відтворені, якщо стан псевдовипадкових чисел відомо.

Для того, щоб отримати щось випадкове, потрібно джерело ентропії, джерело певного хаосу яке буде використовуватись для генерації випадковості.

Це джерело використовується для накопичення ентропії з подальшим отриманням з неї початкового значення (initial value, seed), яке необхідно для формування випадкових чисел у ГВЧ.

Щоб створити псевдовипадкову послідовність потрібен алгоритм, який буде генерувати деяку послідовність на підставі певної формули. Також, важливим моментом є те, де буде реалізовано цей алгоритм. В якості платформи для такого генератора було обрано мікроконтролер.

На даний момент складно уявити будь-яке серйозне обладнання без використання мікроконтролерів (МК). Як відомо, типовий МК виконаний на одному кристалі і містить процесор, периферійні пристрої, ОЗУ (оперативно запам'ятовуючий пристрій) і / або ПЗУ (постійний запам'ятовуючий пристрій), в залежності від призначення. Іншими словами, мікроконтролер можна представити у вигляді міні комп’ютера, здатного вирішувати нескладні обчислювальні завдання.

Мікроконтролер до слова не може генерувати випадкові числа, тому що він точний обчислювальний пристрій і випадковостей в його роботі бути не може.

Головною частиною генератора є МК ATMEGA328P-MU в корпусі MLF-32. Мікроконтролер вже розпаяний на платформі Arduino, що істотно спрощує монтаж і налагодження МК і дозволяє приділити більше уваги розробці самого генератора.

Для розробки власного алгоритму формування псевдовипадкових чисел проаналізуємо готові функції платформи для роботи з псевдовипадковими числами.

random (max); - повертає псевдовипадкове число в діапазоні від 0 до (max - 1). max приймає значення unsigned long, тобто від 0 до 4 294 967 295.

random (min, max); - повертає псевдовипадкове число в діапазоні від min до (max - 1). max приймає значення unsigned long, тобто від 0 до 4 294 967 295

randomSeed (value); - дати генератору псевдовипадкових чисел нову опорну точку для відліку. value - будь-яке число типу unsigned long, значить на Arduino ми маємо 2^{32} (4 294 967 295) наборів псевдовипадкових чисел [4].

Для того, щоб правильно генерувати випадкові числа і щоб послідовність кожного разу була нова, при запуску програми потрібно задавати випадкове число в randomSeed ().

Якщо пристрій якось взаємодіє зі зовнішнім світом або з користувачем, то можна при настанні деяких апаратно випадкових подій (натискання кнопки, спрацьовування датчика, прийняття даних, і т.д.) надавати команді randomSeed даний час з моменту старту програми, тобто функції millis () або micros () [5].

Апаратно випадкові числа можна брати через виводи (піни). Якщо пін нікуди не під'єднано, то він ловить «з повітря» різноманітні наведення радіосигналів. Шуми мають природу близьку до випадкової і цим фактором можна скористатися для формування випадкових подій.

Використовуючи вбудовану функцію відбудови графіків по даним, що надходять у послідовний порт, в програмному середовище Arduino IDE було отримано графік зображений на рис.1.

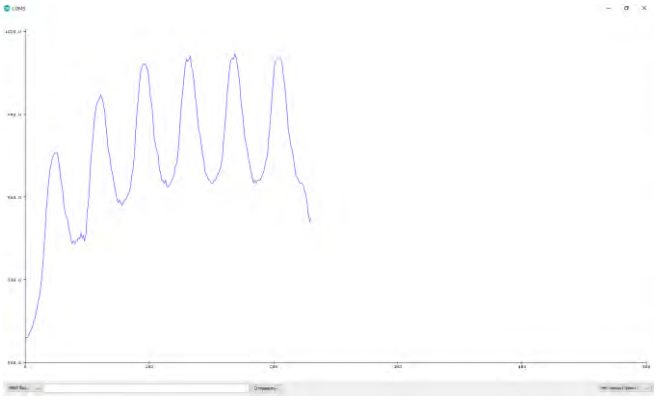
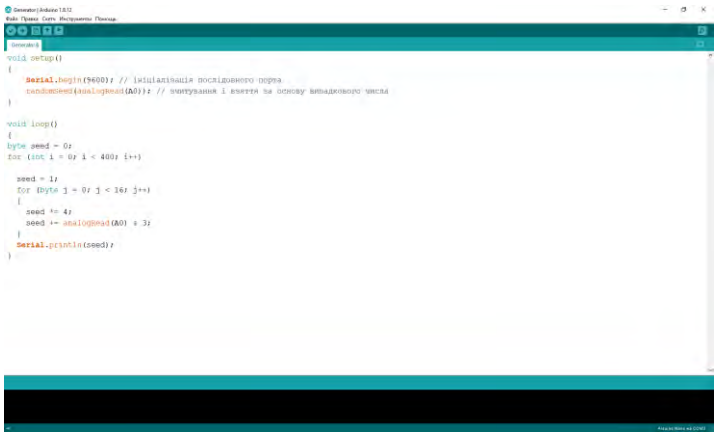


Рис.1. Відбудований графік по значенням з аналогового входу

Як видно з рис.1 сигнал, який зчитується з чистого аналогового входу схожий на синусоїду. Це пояснюється тим, що в стінах будівель є велика кількість провідників з мережевою напругою і вони створюють наводки на мікроконтролер. Ці значення можна використовувати в якості «зерна» для функції randomSeed().

Таким чином, враховуючи вище викладене, було запрограмовано генератор псевдовипадкових чисел на мікроконтролері плати Arduino (рис.2).



```
void setup()
{
  Serial.begin(9600); // ініціалізація послідовного порта
  randomSeed(analogRead(A0)); // зчитування і взяття за основу випадкового числа
}

void loop()
{
byte seed = 0;
for (int i = 0; i < 400; i++)

  seed = 1;
  for (byte j = 0; j < 16; j++)
  {
    seed *= 4;
    seed += analogRead(A0) + 3;
  }
  Serial.println(seed);
}
```

Рис.2. Програмний код генератора псевдовипадкових чисел

В реалізованому програмному коді (рис.2) було обрано тип даних byte (255 можливих значень) замість типу даних unsigned long, оскільки для подальшої реалізації на ЕОМ потік з 4 294 967 295 значень є непотрібним.

Як видно з рис.3 поява значень є випадковою і не прослідковується закономірність.

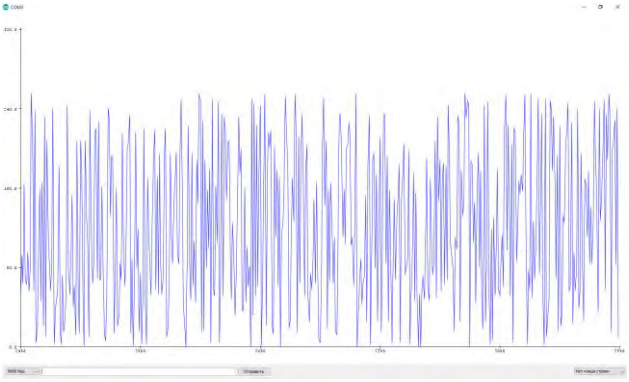


Рис.3. Відбудований по випадковим значеннях генератора графік

Зробимо вибірку значень і побудуємо графік для наглядного бачення розсіювання значень. Для наочності вибірка значень бралася для генератора, що працює з типом даних unsigned long (рис.4).

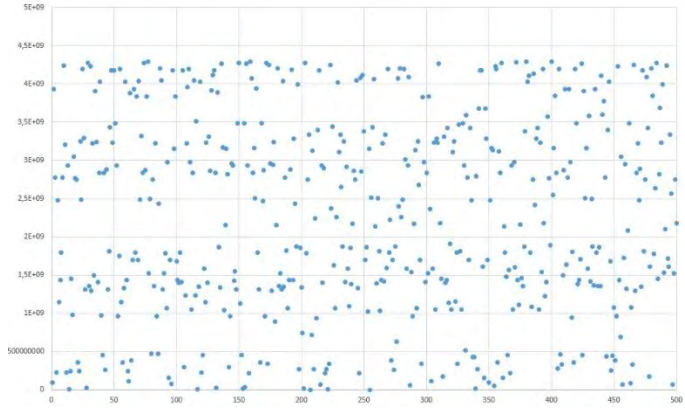


Рис.4. Вибірка значень розробленого генератора чисел

Таким чином, маємо практично рівномірне розсіювання і величезну кількість випадкових значень, отриманих шляхом перемноження і складання шуму.

Для реалізації генератора псевдовипадкових чисел передбаченого структурною схемою розроблюваного пристрою було обрано плату Arduino Pro Mini [6].

Для запису програмного коду і суміщення плати з ЕОМ пропонується використати перехідник USB – TTL [7]. Таким чином, плата Arduino Mini разом з перехідником при під’єднані до ЕОМ буде розмірами з стандартний флеш-накопичувач.

Висновки

Розроблений апаратний генератор псевдовипадкових чисел може виступати основою як для апаратно реалізованих, так і програмно реалізованих генераторів шуму. Використання такого генератора псевдовипадкових чисел дозволить зробити систему стійкою, що підвищить рівень захищеності інформації за рахунок ускладнення фільтрування зловмисниками корисного сигналу серед суміші сигналів. Реалізація на платформі Arduino Pro Mini дає можливість зменшити розміри генератора псевдовипадкових чисел та значно здешевити виробництво генераторів шуму, що в подальшому відобразиться на доступності систем захисту інформації при високих показниках ефективності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Чекатков А.А., Хорошко В.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504 с.

2. Зайцев А.П., Шелупанов А.А, Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защити информации.- Москва: «Машиностроение». -2009 г. – 508 с

3. Рибальський О.В., Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ

МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов – К.: Вид. Національної академії внутрішніх справ, 2012. – 104 с.

4. Соммер У. Программирование микроконтроллерных плат Arduino/Freeduino. — СПб.: БХВПетербург, 2012. — 256 с.: ил. — (Электроника)
5. Perea F. Arduino Essentials. Packt Publishing, 2015. - 206 p., english, ISBN 13: 9781784398569
6. Arduino Pro Mini. URL: https://doc.arduino.ua/ru/hardware/ProMini
7. USB-TTL конвертер PL2303HX USB-UART. URL: https://www.mini-tech.com.ua/usb-uart-converter-na-chipe-pl2303

Сінюгін Вадим Валерійович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця. vadim2804@gmail.com

Катаєв Віталій Сергійович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця. kataev@vntu.net,

Vadym Siniuhin - assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia. vadim2804@gmail.com

Vitaliy Kataev - assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia. kataev@vntu.net