УДК 004.056
DOI: 10.31673/2409-7292.2021.011418

Чечко А.С.

ЗАСТОСУВАННЯ РОЗПОДІЛІВ ДЖОНСОНА ДЛЯ ОПИСУ ШУМІВ В ПРОБЛЕМІ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ЗА РАХУНОК ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ПОЛІВ USB-КЛАВІАТУРИ

В роботі розглянута проблема опису штучно присутніх індустріальних шумів, які є в наявності при експлуатації персональних комп'ютерів. Ці шуми мають як позитивний вплив так і негативний при захисті інформації, яка набирається користувачем засобами клавіатури інтерфейсу USB. Труднощі, які при цьому виникають, пов'язані з тим, що побічне випромінювання електромагнітних полів спостерігається при роботі всіх елементів обчислювальної техніки. З одного боку, наявність цих шумів спотворює корисний сигнал, що в свою чергу не дає зловмиснику виявити достовірну інформацію, яка передається. З іншого боку, ці шуми заважають створити відповідні заходи для забезпечення повного захисту при наборі тексту користувачем персонального комп'ютера. В роботі запропоновано розглядати індустріальні шуми у вигляді трьох випадкових процесів, які описуються розподілами Джонсона.

Ключові слова: побічне електромагнітне випромінювання, сигнал, щільність розподілу, шум, оцінка сигналу, клавіатура інтерфейсу.

Вступ

Для оцінки рівня захищеності інформації від перехоплення за рахунок побічного електромагнітного випромінювання (ПЕМВ) USB клавіатури, необхідно дослідити умови при яких це перехоплення можливо. Захист інформації в даних умовах залежить від параметрів корисного сигналу, та від впливу електромагнітних полів, які присутні при експлуатації персонального комп'ютера, а також від інформації, якою володіє суб'єкт, який здійснює перехоплення. Існує багато методик атестації персональних комп'ютерів та їх компонент, які визначають загрозу витоку інформації за рахунок побічних електромагнітних полів, але вони не враховують особливості побічних електромагнітних полів окремих компонент персональних комп'ютерів. Однією з таких компонент є клавіатура інтерфейсу USB. Однією з характеристик, які створюють відповідні труднощі для виявлення витоку інформації є шум, який уявляє собою деякий випадковий процес. Визначення характеристик цього процесу присвячена дана робота.

Постановка проблеми. Сигнал, який випромінює кабель USB клавіатури, є періодична послідовність імпульсів, які мають певну тривалість, амплітуду, час появи першого імпульсу, затримку між імпульсами. При отриманні оцінки достовірності виявлення та відновлення сигналу побічного електромагнітного випромінювання USB клавіатури та захисту інформації при цих умовах, необхідно враховувати характеристики шумів, які необхідно вилучати. Виходячи з цього, виникає завдання описати всі можливі шуми, які присутні при побічному електромагнітному випромінюванні і визначити їх параметри.

Аналіз публікацій. В роботі [1] розв'язок задачі класифікації аерокосмічних зображень здійснюється за допомогою апроксимації щільності розподілу ознак зображень розподілами Джонсона. Результати, які отримані в даній роботі, а саме формули для багатовимірної щільності розподілу ознак та оцінки її розподілу, отримали застосування до оцінки параметрів шумів, які виникають при побічному електромагнітному випромінюванні клавіатури інтерфейсу USB. В роботі [2] розвинена проблематика появи ПЕМВ при експлуатації електронно-обчислювальної техніки. Дана характеристика каналів витоку інформації за рахунок ПЕМВ, а також розглянута методика вимірювання ПЕМВ. Однак, в даній роботі не враховуються шуми, які виникають в процесі ПЕМВ і які заважають здійсненню точних розрахунків при виборі засобів захисту інформації. В роботі [3] запропонована математична модель виявлення ПЕМВ відеосистеми комп'ютера оптимальним прймачем і яка дає можливість оцінити можливість перехоплення ПЕМВ засобами розвідки. Однак, в даній роботі використовується спектральна щільність шуму, але не вказано, яким чином ця щільність визначається. В роботі [4] здійснено загальний аналіз утворення каналів витоку інформації за рахунок ПЕМВ для різних компонентів комп'ютера.

На основі експериментальних даних підкреслено, що на частотах одиниць ГГц існує небезпечний сигнал. Також відзначено, що наявність ПЕМВ породжує канал витоку мовної інформації компонентами комп'ютера, які обробляють інформацію. Однак, в даній роботі не запропоновано жодної моделі, за допомогою якої можна було б здійснити аналіз методів та засобів захисту інформації від витоку за рахунок ПЕМВ.

Мета статті. Метою даної статті є визначення негаусовських шумів, які виникають при побічному електромагнітному випромінюванні, та обчисленні їх параметрів.

Викладення основного матеріалу. Причиною виникнення побічного електромагнітного випромінювання при роботі електромагнітних пристроїв є наявність диференціальних та синфазних електричних струмів. Одним із способів захисту інформації від ПЕМВ є активне радіотехнічне маскування. Сутність цього маскування полягає в формуванні та випромінюванні маскуючого сигналу на дуже малій відстані від засобу, що захищається [5]. При цьому існують чотири основні методи активного радіотехнічного маскування, які приведені на рисунку 1.

Рис. 1. Основні методи активного радіотехнічного маскування.

Метод білого шуми отримав широке застосування на теперішній час, але недолік його полягає в створені штучних недоступних індустріальних шумів електронними засобами, які знаходяться в приміщенні, де також присутня обчислювальна техніка, що потребує захисту. Спектрально енергетичний метод дозволяє визначити оптимальний шум з обмеженою потужністю для досягнення необхідного співвідношення сигнал/шум на межі контрольованої зони [5]. Вищезазначені два методи можуть використовуватись для захисту інформації як аналогової так і цифрової техніки.

При використанні методу синфазного шуму відбувається повне маскування сигналу шумом і відсутня необхідність в прийомі сигналу, так як апостеріорна ймовірність присутності та відсутності сигналу приймає апріорні значення. В цьому випадку критерієм захищеності є максимальне значення повної ймовірності помилки на границі мінімальної зони доступності.

При використанні статистичного методу в якості контролю характеристик сигналів будуються матриці ймовірностей переходів між можливими станами ПВЕМ. Якщо всі елементи цієї матриці однакові, то це означає, що система оптимальна захищена. Перевага цього методу полягає в тому, що рівень сигналу, який маскується, не перевищує рівень інформативних ПВЕМ обчислювальної техніки.

Шуми, які виникають при ПЕМВ характеризуються видом миттєвої щільності розподілу. Якщо ці шуми істотні, то вони описуються гаусовською щільністю розподілу з двома параметрами – математичним сподіванням і середнім квадратичним відхиленням. Однак, при експлуатації персонального комп'ютера, крім істотних шумів існують штучні, які називають індустріальними. Індустріальні шуми описуються щільністями розподілу, які крім основних параметрів математичного сподівання і середнє квадратичного відхилення, характеризуються ще додатковими двома параметрами – асиметрією і ексцесом. Відомо, що широкий клас індустріальних шумів описуються одним з трьох розподілів Джонсона.

Істотні шуми уявляють собою випадковий процес, який має гаусовський розподіл.

$$f(\xi)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(\xi-M(\xi))^2}{2\sigma^2}}. \qquad (1)$$

Внутрішні шуми приймача мають нормальну щільність розподілу з нульовим математичним сподіванням і одиничним середнім квадратичним відхиленням.

$$f(\varepsilon)=\frac{1}{\sqrt{2\pi}}e^{-\frac{\varepsilon^2}{2}}. \qquad (2)$$

Штучні індустріальні шуми уявляють собою випадковий процес, який можна описати одним з трьох розподілів Джонсона. Сутність цих розподілів полягає в тому, що індустріальний шум уявляє собою випадковий процес, який можна описати на основі гаусовського процесу за рахунок перетворення випадкової величини ξ, яка є змінною в формулі (1). Дослід показує, що індустріальні шуми уявляють собою одним з трьох випадкових процесів. Першим є процес $L(\xi)$, який описується L- перетворенням Джонсона. Це перетворення здійснюється введенням нової випадкової величини, яка має вид

$$X_1=A+E\ln\frac{\xi-M(\xi)}{\sigma}, \qquad (3)$$

де A, E - невідомі параметри, які характеризують особливості індустріальних шумів. Тоді, закон розподілу, який описує випадковий процес $L(\xi)$, має вид

$$f(\xi,X_1)=\frac{E}{(\xi-M(\xi))\sqrt{2\pi}}e^{-\frac{1}{2}E^2\left(\frac{A}{E}+\ln\frac{\xi-M(\xi)}{\sigma}\right)^2}. \qquad (4)$$

На рисунку 2 зображено графік щільності розподілу випадкового процесу $L(\xi)$.

З рисунку 2 видно, що параметр E уявляє собою ексцес, а параметр A- асиметрію L - розподілу Джонсона.

Другий закон розподілу, який описує випадковий процес $B(\xi)$, отримується за допомогою випадкової величини, яка має вид

$$X_2=A+E\ln\frac{\xi-M(\xi)}{\sigma-\xi+M(\xi)}. \qquad (5)$$

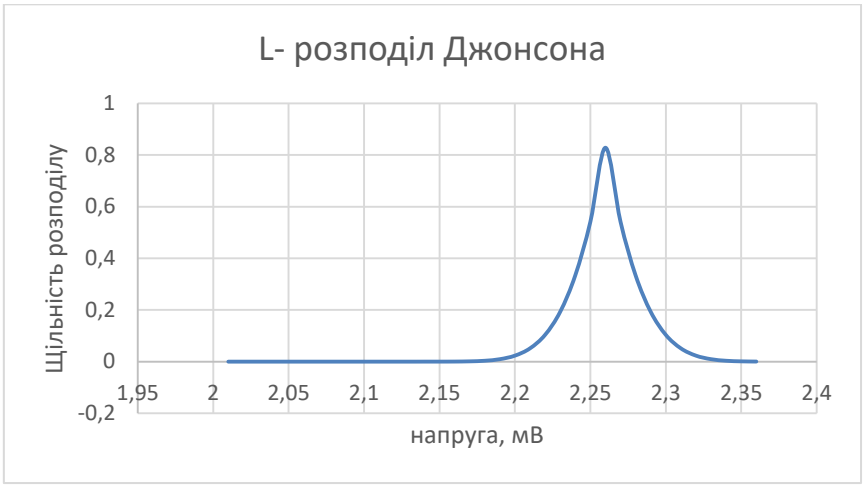

Рис.2. Графік щільності (4) при $E=5,\ A=1,\ M(\xi)=2,\ \sigma=0.5$.

В цьому випадку, маємо

$$f(\xi, X_2)=\frac{E\sigma}{(\xi-M(\xi))(\sigma-\xi+M(\xi))}e^{-\frac{1}{2}E^2\left(\frac{A}{E}+\ln\left(\frac{\xi-M(\xi)}{\sigma-\xi+M(\xi)}\right)\right)^2}. \quad (6)$$

Реалізація третього випадкового процесу Джонсона $U(\xi)$ здійснюється за рахунок введення випадкової величини X_3, яка є перетворенням випадкової величини ξ, яке має вид

$$X_3=A+E\ln\left(\frac{\xi-M(\xi)}{\sigma}+\sqrt{1+\left(\frac{\xi-M(\xi)}{\sigma}\right)^2}\right). \quad (7)$$

Закон розподілу, що описує випадковий процес $U(\xi)$ з урахуванням (7), має вид

$$f(\xi, X_2)=\frac{E}{\sqrt{2\pi\left(\sigma^2+(\xi-M(\xi))^2\right)}}e^{-\frac{1}{2}E^2\left(\frac{A}{E}+\ln\left(\frac{\xi-M(\xi)}{\sigma}+\sqrt{1+\left(\frac{\xi-M(\xi)}{\sigma}\right)^2}\right)\right)^2}. \quad (8)$$

За допомогою експериментальних стендів лабораторії Кафедри систем інформаційного та кібернетичного захисту Навчально наукового інституту захисту інформації Державного університету телекомунікацій були проведені експерименти виявлення індустріальних шумів при побічному випромінюванні побічних електромагнітних полів інтерфейсу клавіатури USB. В результаті було здійснено відповідні виміри з порівнянням гаусовських розподілів і розподілів Джонсона. Результати аналізу приведені в таблиці 1.

Результати отриманих вимірювань, які приведені в таблиці 1 дають можливість стверджувати, що невідомі параметри, які присутні в розподілі випадкових процесів Джонсона $L(\xi), B(\xi)$ і $U(\xi)$ наближенні до асиметрії - параметр A та ексцесу – параметр E.

Висновок. При побічному випромінюванні електромагнітних полів присутні штучні індустріальні шуми, які уявляють випадкові процеси. Ці перешкоди відіграють як позитивну роль, так і негативну. Позитивність їх полягає в тому, що вони спотворюють корисний

сигнал, що в свою чергу не дають можливість здійснювати контроль за наявністю несанкціонованого доступу до інформації за рахунок цього випромінювання. З іншого боку, ці шуми не дають можливість контролювати повний захист інформації, що передається засобами інтерфейсу клавіатури USB. Ці процеси на практиці достатньо складно описати. Однак, при введенні двох параметрів, а саме асиметрії і ексцесу розподілу, можна за рахунок їх коригування керувати процесом захисту інформації від її витоку за рахунок побічного випромінювання електромагнітних полів.

Таблиця 1.

Результати вимірювань побічних електромагнітних полів інтерфейсу USB клавіатури

Розподіл	Середня потужність шуму/середня потужність корисного сигналу, в децебелах	$M(\xi)$ - середня амплітуда сигналу, що в результаті прийнятий, в мВ	σ^2 - середнє квадратичне відхилення амплітуди сигналу, в $мВ^2$	A безрозмірна величина	E безрозмірна величина	Коефіцієнт кореляції безрозмірна величина
$f(\xi)$	-15…20	0	0.2	0	0.5	0
$f(\xi, X_1)$	-15…20	-1	0.2	0	0.5	0
$f(\xi, X_2)$	-15…20	-0.5	0.2	0	0.5	0
$f(\xi, X_3)$	-15…20	0	0.2	0	0.5	0
$f(\xi)$	-15…20	0	1	0	1	0
$f(\xi, X_1)$	-15…20	-1	1	0	1	0
$f(\xi, X_2)$	-15…20	-0.5	1	1	1	0
$f(\xi, X_3)$	-15…20	0	1	1	1	0
$f(\xi)$	-15…20	-1	5	0	2	0.9
$f(\xi, X_1)$	-15…20	-0.5	5	0	2	0.9
$f(\xi, X_2)$	-15…20	0	5	2	2	0.9
$f(\xi, X_3)$	-15…20	0	5	2	2	0.9

Перелік посилань

1. Ю.Б. Буркатовская, «Применение распределений Джонсона к задаче классификации аэрокосмических изображений» / Ю.Б. Буркатовская, Н.Г. Марков, А.С. Морозов, А.П. Серых. Известия Томского политехнического университета. Т. 311. №5, сс. 76-80, 2007.

2. В.Б. Дудикевич, «Дослідження побічного електромагнітного випромінювання від флеш носіїв» / В.Б. Дудикевич, І.С. Собчук, Л.М. Ракобовчук, В.С. Зачепило. Системи обробки інформації. Випуск 3(93), сс. 112-116, 2011.

3. А.А. Хорев, «Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера», Доклады ТУСУРа, №2(32), сс. 207-212, июнь 2014.

4. Ю.І. Хлапонін, «Особливості виникнення каналу витоку інформації за рахунок побічного електромагнітного випромінювання і наведення», Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, Вип.2 (3), сс. 58-63, 2015.

5. Ластівка Г.І., Шпатар П.М., «Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник» - Чернівці: Чернівецький національний університет, 2018. – 252 с.

Надійшла: 22.01.2021 Рецензент: д.т.н., професор Савченко В.А.