УДК 621.396 **DOI:** 10.31673/2412-9070.2020.046167

Л. П. КРЮЧКОВА, доктор техн. наук, доцент;
А. Г. ЗАХАРЖЕВСЬКИЙ, здобувач;
О. С. ЛАЗУТІН, магістр;
Є. О. УКРАЇНЕЦЬ, магістр;
С. В. ПАНАДІЙ, здобувач,
Державний університет телекомунікацій, Київ

ДОСЛІДЖЕННЯ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ІНТЕРФЕЙСУ USB У СИСТЕМІ КЕРУВАННЯ ІНФОКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

Розглянуто процеси формування технічних каналів витоку інформації побічними електромагнітними випромінюваннями під час використання USB-інтерфейсу в структурі системи керування інформаційно-комунікаційними мережами. Наведено зображення рівнів сигналів побічних електромагнітних випромінювань інтерфейсу USB 2.0, отриманих за допомогою аналізатора спектра ROHDE&SCHWARZ FSW 13 (Signal & Spectrum Analyzer) із використанням антени R&S Active Dipole Antenna HE527.

Ключові слова: побічні електромагнітні випромінювання; цифрові системи передавання; електромагнітне поле; послідовні шини; USB-інтерфейс.

Вступ

Одним із ключових напрямків розвитку сучасного суспільства є формування інтегрованого інформаційного простору на основі новітніх інформаційних технологій. Широке застосування інформаційних технологій і інфокомунікаційних мереж (ІКМ) для передавання, приймання, оброблення та зберігання інформації в різних сферах діяльності, з одного боку, сприяє підвищенню ефективності цієї діяльності, а з другого — зумовлює виникнення загроз витоку інформації технічними каналами, під якими розуміється неконтрольоване поширення інформативного сигналу від його джерела через фізичне середовище до технічного засобу, який здійснює перехоплення інформації.

У процесі боротьби за інформацію сторони реалізують найрізноманітніші заходи щодо її «руйнування», «спотворення», «приховування» і «вилучення» під час конфліктної взаємодії систем, здійснюваній за допомогою передавання та приймання випромінювань у діапазоні електромагнітних хвиль. Взаємний вплив, що призводить до зміни інформаційних станів об'єктів, здійснюється, як правило, безконтактним способом на основі електромагнітних полів, що виконують функцію переносника інформації і поширюються у фізичному середовищі. До конфліктної взаємодії залучаються інформаційні системи всіх відомих класів: передавання і перехоплення інформації, радіокерування і руйнування інформації. Ці системи функціонують у всіх освоєних нині діапазонах хвиль і використовують усі відомі в технічних застосуваннях фізичні поля. Усі вони стають учасниками інформаційного радіоелектронного конфлікту.

Створення комплексів дестабілізуючих впливів пов'язано з інтеграцією класичних засобів радіоелектронного придушення, засобів інформаційно-технічного впливу, а також засобів радіомоніторингу та комп'ютерної розвідки. Деструктивні впливи спрямовуються на руйнування інформаційних потоків, що циркулюють між елементами мережі; зменшення швидкості інформаційного обміну між елементами системи керування, істотно збільшуючи тривалість циклу керування і, як наслідок, знижуючи ефективність керування мережею; забезпечення достатньо масованого і довготривалого виведення з ладу мережних технічних засобів. Існує принципова можливість створення нових видів впливів, що реалізують приховане функціональне ураження системи зв'язку завдяки створенню і розвитку внутрішньосистемних суперечностей між її окремими протоколами [1].

Керування інфокомунікаційними мережами, які функціонують у складних зовнішніх умовах, є важливою проблемою як з позиції розроблення системи керування, так і з погляду реалізації керування в процесі функціонування інфокомунікаційної мережі [2].

Процеси керування в системі керування інфокомунікаційною мережею — це інформаційний процес, який можна подати як сукупність цілеспрямованих операцій збору і оброблення інформації, прийняття рішень, доведення рішень до об'єктів керування, а також контролю виконання вироблених рішень. Важливість інформації, а також вимога забезпечення стійкості функціонування зумовлюють необхідність включення до складу інфокомунікаційних систем захисних підсистем, призначених для нейтралізації впливів факторів зовнішнього середовища.

Організація інтегрованого керування сучасними ІКМ потребує застосування відповідних програмно-апаратних платформ, які забезпечують необхідний рівень якості послуг зв'язку в будь-який час і з мінімальними експлуатаційними витратами. Вирішення задачі досягається створенням спеціальної мережі керування, яка забезпечує керування ІКМ і послугами завдяки організації взаємозв'язку з компонентами різних систем зв'язку на основі єдиних інтерфейсів і протоколів (такий підхід застосовується в концепції **TMN** (*Telecommunications Management Network*), прийнятої МСЕ-Т).

Для попередження і нейтралізації інцидентів інформаційної безпеки потрібно як комплексне застосування захисних заходів, так і випереджальні науково-технічні розробки. Останні потребують всебічного дослідження причин появи зазначених інцидентів — уразливостей мереж.

У переліку загроз ІКМ важливе місце посідають загрози витоку інформації каналами побічних електромагнітних випромінювань (ПЕМВ), а також унаслідок наведень інформаційних сигналів у лініях електроживлення технічних засобів оброблення інформації, сполучних лініях допоміжних технічних засобів і систем, колах заземлення і сторонніх провідниках. У зарубіжній літературі замість терміна ПЕМВ використовуються терміни «*compromising electromagnetic emanations*» (компрометуючі електромагнітні випромінювання) або TEMPEST (скорочення від «*transient electromagnetic pulse emanation standard*» — стандарт на електромагнітні імпульсні випромінювання, спричинені перехідними процесами в електронній апаратурі).

Проблема витоку конфіденційної інформації каналами побічних випромінювань і наведень (ПЕМВН) інтенсивно досліджується з 1985 року, після першої відкритої наочної демонстрації цього способу перехоплення інформації голландським інженером Вімом ван Ейком (Wim van Eck) [3].

Дослідження проводяться за двома напрямками:

1) вирішення задач, які виникають під час перехоплення інформативних сигналів та вилучення з них конфіденційної інформації (задачі перехоплення);

2) вирішення задач, які постають у процесі організації захисту конфіденційної інформації від витоку (задачі захисту).

До складу системи керування ІКМ входять USB-інтерфейси, які забезпечують передавання даних між системними блоками засобів обчислювальної техніки та периферійними пристроями [4].

Історія інтерфейсу *Universal Serial Bus* (USB), який сьогодні є де-факто стандартом для периферійних пристроїв, веде свій початок із 1994 року. Консорціум розробників складався з семи компаній: Compaq, DEC, IBM, Intel, Microsoft, NEC і Nortel, головним розробником був співробітник Intel Аджай Бхатт (Ajay Bhatt). Підґрунтям до створення нової технології стала зростаюча потреба в зручному інтерфейсі для підімкнення периферійних пристроїв, оскільки типові для тих років COM, LPT і PS/2 мали низьку пропускну здатність і не підтримували гаряче підімкнення, а їхні розніми були незручні для застосування через великі розміри, зумовлені великою кількістю контактів.

Застосування інтерфейсу USB дає можливість швидко під'єднувати необхідні блоки для автоматизації об'єктів керування і контролю. Просте і гнучке програмне забезпечення дає змогу розробнику написати програму керування зовнішнім об'єктом (для комп'ютера: C++, C++ Builder, для контролера: Assembler, C). Гальванічна розв'язка забезпечує електричну сумісність об'єкта керування і комп'ютера, підвищує надійність системи.

Перевага послідовних USB-інтерфейсів порівняно з паралельними інтерфейсами полягає ще й у тому, що в них відсутнє явище перекосу (skew), яке істотно знижує досяжну межу тактової частоти. Перекіс у паралельних інтерфейсах обмежує і допустиму довжину інтерфейсних кабелів [5].

Для захисту інформації від її витоку за рахунок побічних електромагнітних випромінювань із комунікацій, що з'єднують системні блоки засобів обчислювальної техніки з периферійними пристроями, важливим є аналіз формування даних сигналів і випромінювань.

У статті викладено результати дослідження побічних електромагнітних випромінювань інтерфейсу USB 2.0, виконаних для вирішення задач оцінювання захищеності інформації на об'єктах інформаційної діяльності.

Основна частина

Передавання даних в USB є однонапрямленим, за потреби передавання даних в обох напрямах контролер по черзі встановлює канал зв'язку у висхідному і низхідному напрямах.

USB 2.0 підтримує три режими роботи: Low-Speed (1,5 Мбіт/с), Full-Speed (12 Мбіт/с) і High-Speed (480 Мбіт/с). На практиці продуктивність нижча: по-перше, використовується надлишкове кодування даних (на вісім «корисних» бітів передається 10), по-друге, є втрати на оброблення протоколу. Реальні значення для High-Speed рідко перевищують 30…35 МБ/с (240…280 Мбіт/с).

USB-контролер має один стандартний кабель для будь-яких периферійних пристроїв, що забезпечує легкість підімкнення і зниження вартості систем. Кабель USB складається з чотирьох жил: +5 В, «земля» і кручена пара для передавання даних. У кабелях mini- і micro-USB використовується п'ята жила для визначення типу розніму (у micro-A вона заземлена, у micro-B — ні). Максимальна теоретична довжина під час використання звичайних проводів становить 5 м, проте на практиці для стійкого з'єднання рекомендуються більш короткі кабелі, найчастіше — до 1,2 м.

Кожний порт USB забезпечує максимальний живильний струм до 500 мА по лінії 5 В, тобто пікова споживана потужність пристрою може становити 2,5 Вт.

Існують дві основні методики оцінювання захищеності інформації від витоку каналами ПЕМВН. Методика спеціальних досліджень, результатом застосування якої є визначення значень радіуса зони $R2$ навколо технічного засобу (ТЗ), на межі і за межами якої напруженість електромагнітного поля інформативного сигналу не перевищує нормованого значення, радіуса зони $r1$ навколо ТЗ, у межах якого не допускається розміщення зосереджених антен, і радіуса зони $r1'$ навколо ТЗ, у межах якого не допускається розміщення випадкових антен. Результатом другої методики оцінювання захищеності інформації є виміряне і розраховане відношення сигнал/шум на межі контрольованої зони.

Для об'єктних досліджень найбільш об'єктивною визнається методика спеціальних досліджень (визначення $R2$, $r1$ і $r1'$), доповнена методом реальних зон. Яку методику застосовувати в кожному конкретному випадку — вибір за фахівцем.

Усі методи на першому етапі передбачають отримання двох панорам сигналів: із вимкненим тестовим сигналом і з увімкненим тестовим сигналом.

Структурну схему експериментальної установки наведено на рис. 1.

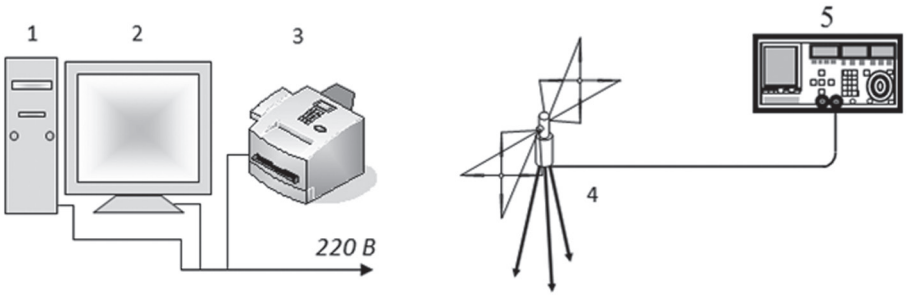

Рис. 1. Структурна схема експериментальної установки:
***1* — системний блок; *2* — монітор; *3* — принтер; *4* — вимірювальна антена; *5* — аналізатор спектра**

Дослідження проводились за допомогою аналізатора спектра ROHDE&SCHWARZ FSW 13 (Signal & Spectrum Analyzer) (рис. 2) із використанням антени R&S Active Dipole Antenna HE527 (рис. 3) та USB флеш-нагромаджувача Transcend J32 2GB.

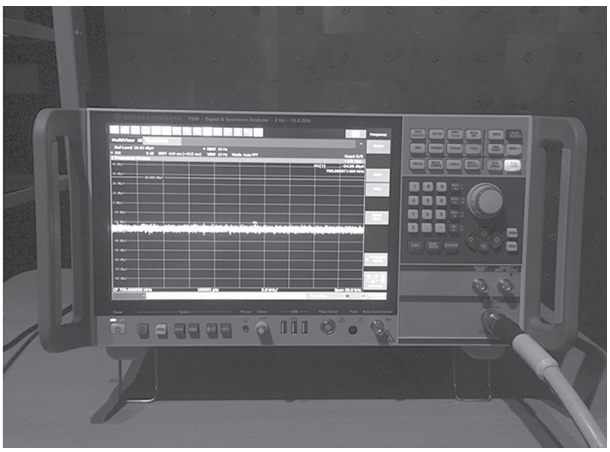

Рис. 2. Зовнішній вигляд аналізатора спектра ROHDE&SCHWARZ FSW 13 (Signal & Spectrum Analyzer)

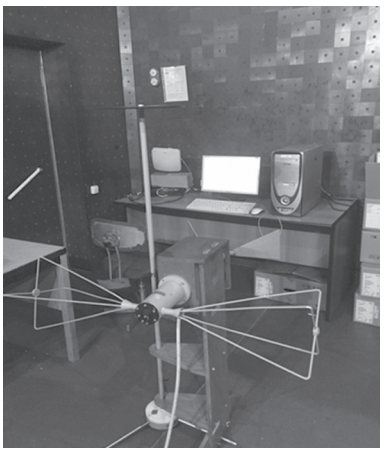

Рис. 3. Зовнішній вигляд дипольної антени R&S Active Dipole Antenna HE527

Зображення сигналів побічних електромагнітних випромінювань інтерфейсу USB 2.0 для різних частот із вимкненим та увімкненим тестовими сигналами подано на рис. 4 – рис. 11.

Рівні сигналів наведено в таблиці.

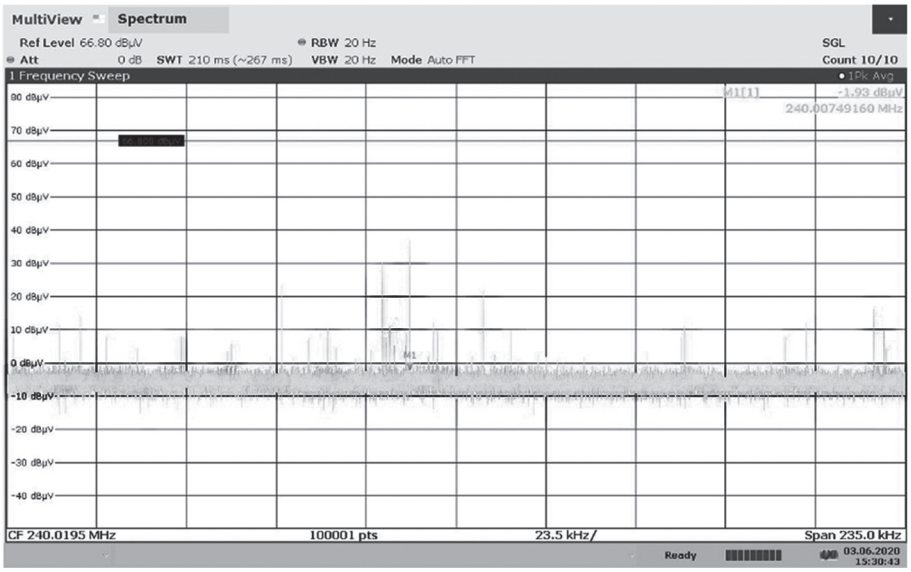

Рис. 4. Рівень сигналу інтерфейсу USB 2.0 із вимкненим тестовим сигналом, де F = 240 MHz, U = −1,93 dBµV

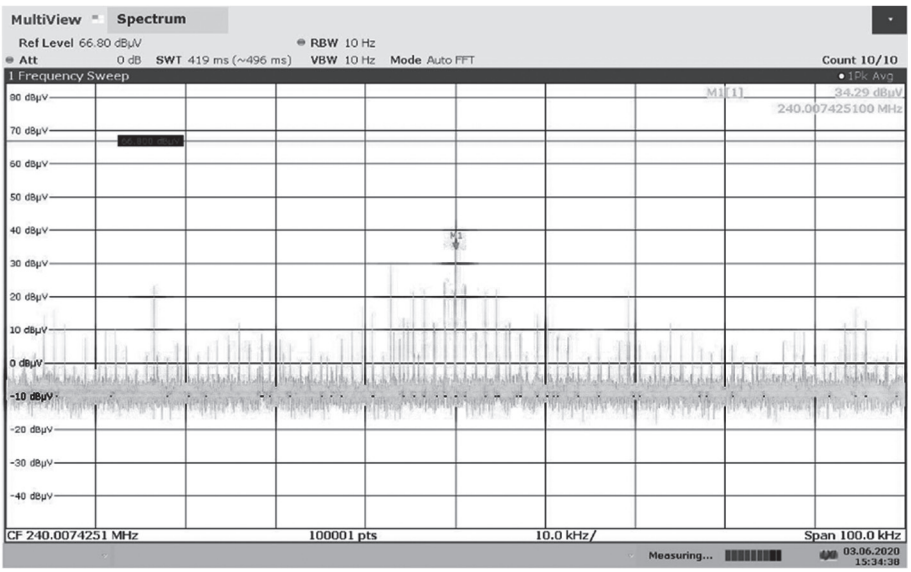

Рис. 5. Рівень сигналу інтерфейсу USB 2.0 із увімкненим тестовим сигналом, де F = 240 MHz, U = 34,29 dBµV

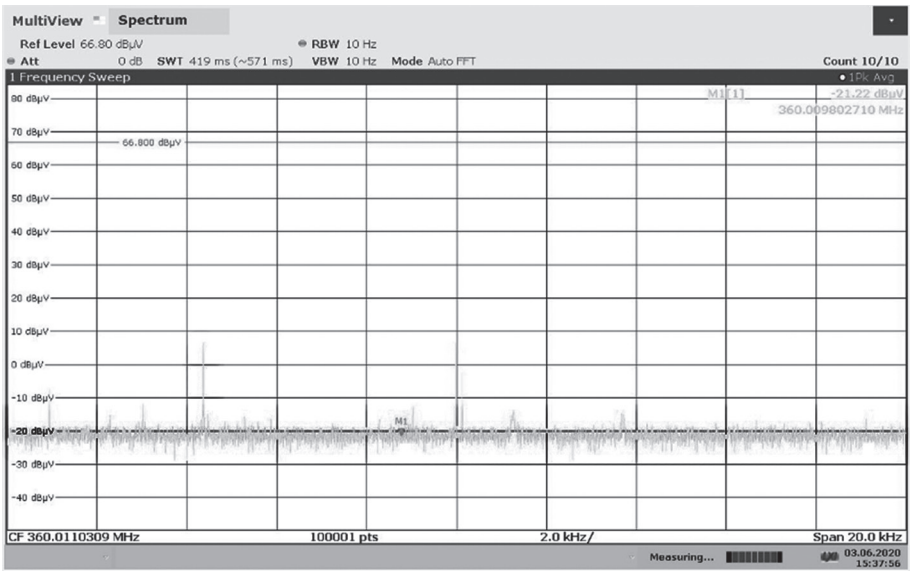

Рис. 6. Рівень сигналу інтерфейсу USB 2.0 із вимкненим тестовим сигналом, де F = 360 MHz, U = −21,22 dBµV

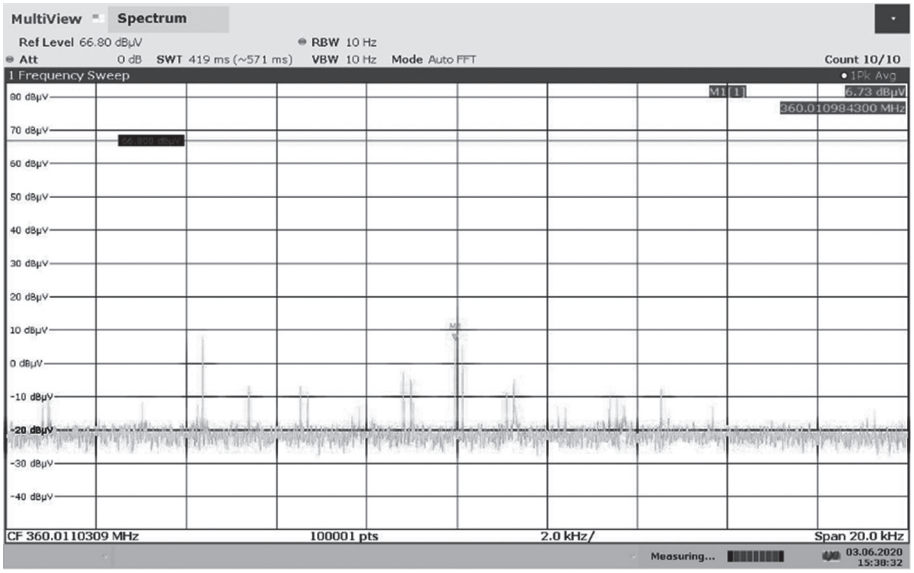

Рис. 7. Рівень сигналу інтерфейсу USB 2.0 із увімкненим тестовим сигналом, де F = 360 MHz, U = 6,73 dBµV

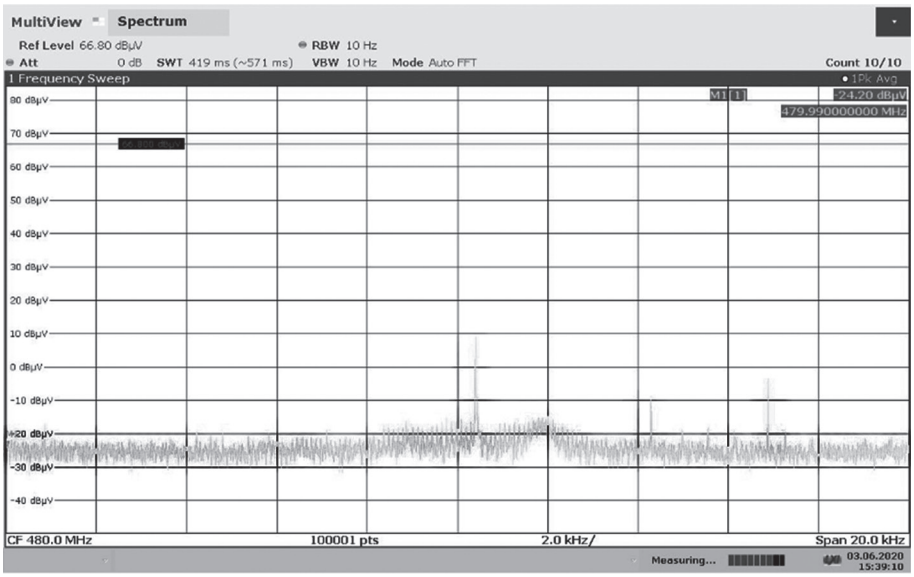

Рис. 8. Рівень сигналу інтерфейсу USB 2.0 із вимкненим тестовим сигналом, де F = 480 MHz, U = −24,20 dBµV

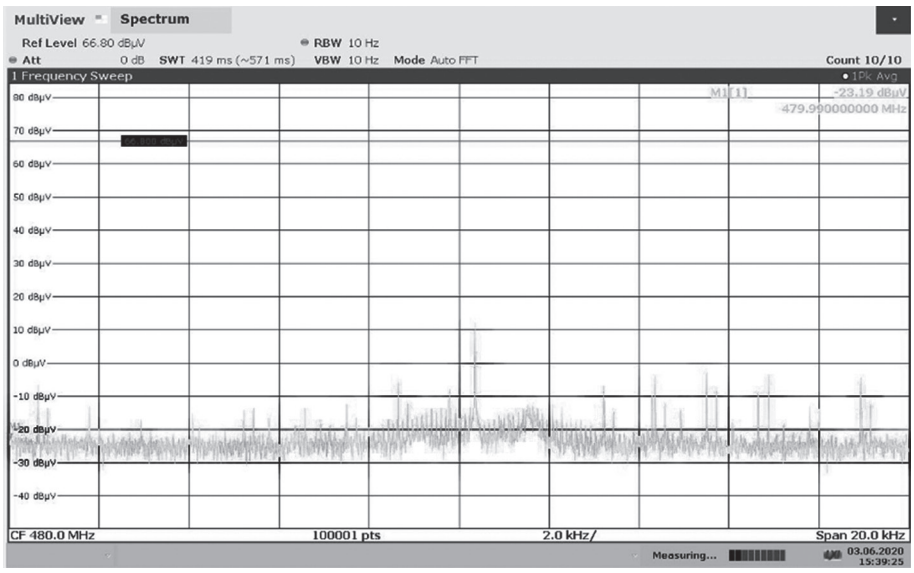

Рис. 9. Рівень сигналу інтерфейсу USB 2.0 із увімкненим тестовим сигналом, де F = 480 MHz, U = −23,19 dBµV

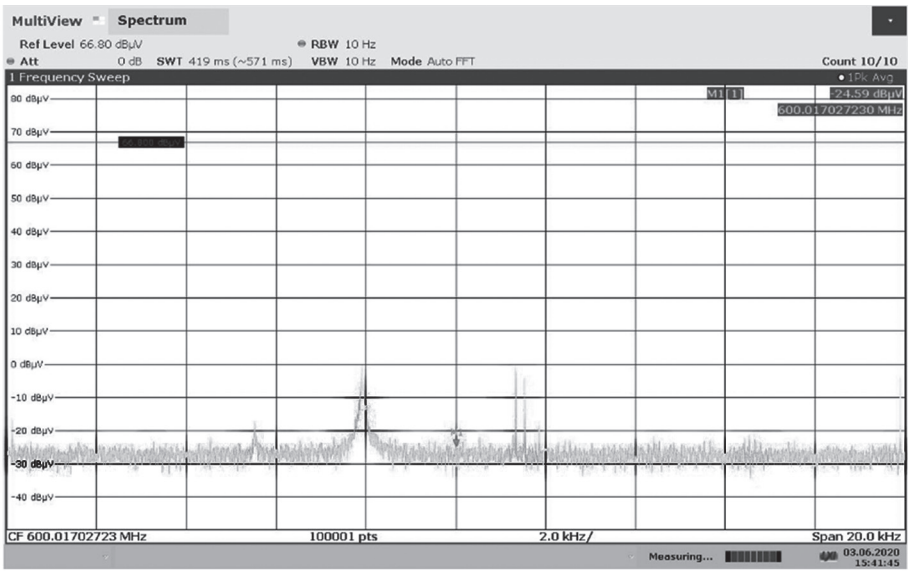

Рис. 10. Рівень сигналу інтерфейсу USB 2.0 із вимкненим тестовим сигналом, де F = 600 MHz, U = −24,59 dBµV

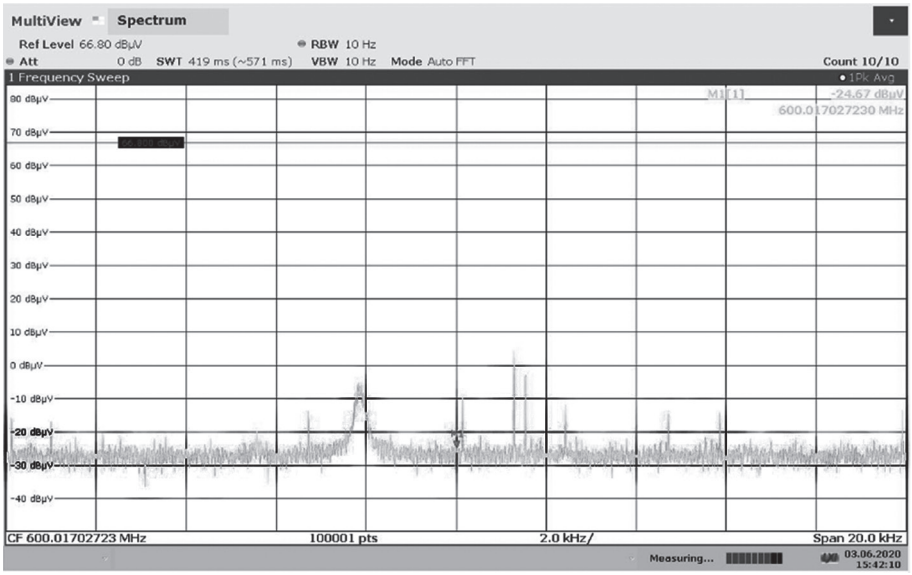

Рис. 11 – Рівень сигналу інтерфейсу USB 2.0 із увімкненим тестовим сигналом, де F = 600 MHz, U = −24,67 dBµV

Рівні сигналів побічних електромагнітних випромінювань інтерфейсу USB 2.0 для різних частот із вимкненим та увімкненим тестовими сигналами

№	Тактова частота, MHz	Рівень сигналу з вимкненим тестом, dBµV	Рівень сигналу з увімкненим тестом, dBµV
1	240,0074251	−1,93	34,29
2	360,0110309	−21,22	6,73
3	480,00000	−24,20	−23,19
4	600,01702723	−24,59	−24,67

Висновки

У результаті аналізу форми і спектра сигналів у кабелі USB (тестовий режим вимкнено, тестовий режим увімкнено) встановлено, що в USB-інтерфейсі постійно відбувається передавання службових пакетів для підтримання інтерфейсу. Під час увімкнення тестового режиму на спектрограмі з'являються додаткові послідовності імпульсів. Частота першої гармоніки для інтерфейсу USB 2.0 перебуває в діапазоні 240 МГц.

Список використаної літератури

*1. **Макаренко С. И.** Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122–185.*

*2. **Стеклов В. К., Костік Б. Я., Беркман Л. Н.** Сучасні системи керування в телекомунікаціях / за ред. В. К. Стеклова. Київ: Техніка, 2005. 395 с.*

*3. **Wim** van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? [Электронный ресурс]. URL:*

http://cryptome.org/emr.pdf вільний (дата звернення: 03.12.2019 р.).

*4. **Universal** Serial Bus, Revision 2,0, April 27, 2000. 570 с.*

*5. **Яшкардин В.** USB. Universal Serial Bus Specification. Универсальная последовательная шина [Электронний ресурс]. URL:*

http://www.softelectro.ru/interface.html вільний (дата звернення: 10.03.2020 г.).

Л. П. Крючкова, А. Г. Захаржевский, А. С. Лазутин, Е. А. Украинец, С. В. Панадий

ИССЛЕДОВАНИЕ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ИНТЕРФЕЙСА USB В СИСТЕМЕ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫМИ СЕТЯМИ

Рассмотрены процессы формирования технических каналов утечки информации побочными электромагнитными излучениями при использовании USB-интерфейса в структуре системы управления информационно-коммуникационными сетями. Приведены изображения уровней сигналов побочных электромагнитных излучений интерфейса USB 2.0, полученных с помощью анализатора спектра ROHDE & SCHWARZ FSW 13 (Signal & Spectrum Analyzer) с использованием антенны R & S Active Dipole Antenna HE527.

Ключевые слова: побочные электромагнитные излучения; цифровые системы передачи; электромагнитное поле; последовательные шины; USB-интерфейс.

L. P. Kryuchkova, A. G. Zakharzhevskyi, O. S. Lazutin, E. O. Ukrainets, S. V. Panadyi

RESEARCH OF COMPROMISING USB INTERFACE ELECTROMAGNETIC EMANATIONS IN THE INFOCOMMUNICATION NETWORKS CONTROL SYSTEM

One of the key directions in the development of modern society is the formation of an integrated information space based on the latest information technologies. The widespread use of information technologies and infocommunication networks for the transmission, reception, processing and storage of information in various fields of activity, on the one hand, contributes to an increase in the efficiency of this activity, and on the other hand, it causes the emergence of threats of information leakage through technical channels, which are understood as the uncontrolled dissemination of information signal from its source through the physical environment to a technical means that intercepts information.

In the list of threats, an important place is occupied by threats of information leakage through channels of compromising electromagnetic emanations, as well as a result of interference of information signals in power lines of technical means of information processing, connecting lines of auxiliary technical means and systems, ground circuits and extraneous conductors.

To protect information from its leakage due to compromising electromagnetic emanations through communications connecting the system blocks of computing facilities with peripheral devices, it is important to analyze the formation of these signals and emissions.

The article presents the results of the study of compromising electromagnetic emanations of the USB 2.0 interface, carried out to solve the problems of assessing the security of information at the objects of information activity. The processes of formation of technical channels of information leakage by compromising electromagnetic emanations at use of the USB-interface in structure of control system of information and communication networks are considered. The images of the signal levels of the compromising electromagnetic emanations of the USB 2.0 interface obtained with the spectrum analyzer ROHDE & SCHWARZ FSW 13 (Signal & Spectrum Analyzer) using the R & S Active Dipole Antenna HE527 are shown.

As a result of the analysis of the form and spectrum of signals in the USB cable (test mode is off, test mode is on) it is established that in the USB interface there is a constant transmission of service packets to support the interface. When the test mode is turned on, additional pulse sequences appear on the spectrogram. The frequency of the first harmonic for the USB 2.0 interface is in the region of 240 MHz.

Keywords: compromising electromagnetic emanations; digital transmission systems; electromagnetic field; serial buses; USB interface.