УДК 004.3.056:621.391.82

К. В. Пугачева
І. О. Бондаренко

АНАЛІЗ СТІЙКОСТІ ЕЛЕКТРОННИХ СХЕМ ДО ЕЛЕКТРОМАГНІТНИХ ІМПУЛЬСНИХ АТАК

Вінницький національний технічний університет

Анотація

У роботі проаналізовано проблематику вразливості сучасних цифрових систем та апаратних засобів до навмисних електромагнітних імпульсних атак (IEMI). Розглянуто механізми виникнення апаратних збоїв на фізичному рівні, таких як «м'які помилки» (bit-flips), фазове тремтіння тактових генераторів та хибне спрацьовування кіл скидання мікроконтролерів під дією наносекундних надширокосмугових імпульсів. Доведено неефективність суто програмних методів кібербезпеки проти таких загроз. Запропоновано комплексний підхід до забезпечення апаратної стійкості, що базується на вимогах стандартів електромагнітної сумісності (ДСТУ IEC 61000-4-2) і включає оптимізацію топології багатошарових друкованих плат, локальне екранування критичних вузлів та застосування швидкісної компонентної фільтрації.

Ключові слова: навмисні електромагнітні атаки, IEMI, електромагнітна сумісність, апаратна безпека, екранування друкованих плат, м'які помилки, TVS-діоди.

Abstract

The paper analyzes the vulnerability of modern digital systems and hardware to intentional electromagnetic interference (IEMI) attacks. The mechanisms of hardware failures at the physical level, such as soft errors (bit-flips), clock generator phase jitter, and false triggering of microcontroller reset circuits under the influence of nanosecond ultra-wideband pulses, are considered. The inefficiency of purely software cybersecurity methods against such threats is proven. A comprehensive approach to ensuring hardware resilience is proposed, based on the requirements of electromagnetic compatibility standards (IEC 61000-4-2), which includes the optimization of multilayer printed circuit board topology, local shielding of critical nodes, and the use of high-speed component filtering.

Keywords: intentional electromagnetic attacks, IEMI, electromagnetic compatibility, hardware security, PCB shielding, soft errors, TVS diodes.

Вступ

Безперервний процес мініатюризації компонентної бази зумовлює до стрімкого розвитку інформаційно-комунікаційних технологій та мікроелектроніки. Зменшення топологічних норм виробництва напівпровідників, підвищення робочих частот та суттєве зниження номінальних напруг живлення цифрових інтегральних схем, окрім позитивних наслідків, спричиняє критичне зниження запасу завадостійкості електронної апаратури. У результаті навіть незначні зовнішні електромагнітні збурення здатні індукувати напруги, що перевищують порогові значення логічних рівнів.

Захист електромагнітної сумісності полягав у захисті обладнання від природних явищ або індустріальних завад. Проте сьогодні дедалі популярнішими стають кіберфізичні загрози – навмисні електромагнітні імпульсні атаки (IEMI – Intentional Electromagnetic Interference). Зловмисники використовують генератори надширокосмугових електромагнітних імпульсів або імітатори електростатичних розрядів для дистанційного впливу на критично важливі вузли. Програмні засоби захисту такі як, алгоритми шифрування, брандмауери, системи контролю доступу та шифрування, є неефективними проти атак на апаратному рівні. За допомогою високоенергетичного імпульсу, який здатний проникати в систему через незахищені інтерфейси дозволяє атакуючій стороні провокувати збої в циклах шифрування для вилучення секретних ключів, обходити механізми автентифікації або повністю виводити обладнання з ладу. Актуальність роботи зумовлена необхідністю перенесення акцентів у захисті інформаційних систем з суто програмного на апаратно-конструктивний рівень.

Результати дослідження

EMC (електромагнітна сумісність) – це здатність електронних та електричних пристроїв працювати в навколишньому середовищі, при цьому не створюючи небажаних електромагнітних завад і не піддаючись впливу небажаних електромагнітних завад [1]. Завади, які мають вплив на електронну апаратуру

класифікують за шляхами їх проникнення на кондуктивні (поширюються струмопровідними колами, зокрема лініями живлення, передачі даних та заземлення) та випромінювані (поширюються у просторі у вигляді електромагнітних хвиль) [2].

На апаратному рівні імпульсні атаки часто реалізуються двома методами: через генерацію надширокосмугових електромагнітних імпульсів просторового випромінювання або шляхом безпосередньої інжекції потужних струмових імпульсів в інтерфейси чи металеві елементи корпусу пристрою. Відмінною рисою таких деструктивних впливів є не стільки сумарна енергія імпульсу, скільки надвисока швидкість наростання його фронту та пікова амплітуда.

Відповідно до вимог стандарту ДСТУ IEC 61000-4-2:2008 типовий тестовий імпульс струму характеризується коротким часом наростання фронту (від 0,7 до 1 наносекунди). Амплітуда напруги такого впливу може сягати 8 кВ у разі контактного розряду та до 15 кВ при повітряному пробої [4]. Такі параметри перетворюють імпульс на потужне джерело високочастотних гармонік, спектр яких простягається до гігагерцового діапазону, що має катастрофічні наслідки для незахищеної апаратури. Високочастотна енергія атаки здатна легко долати гальванічну розв'язку та проникати у внутрішні кола через паразитні ємності та індуктивності мікросмугових ліній друкованої плати [3]. Низькочастотні RC- та LC-фільтри виявляються інерційними і майже непомітними для таких наносекундних сплесків. Це дозволяє імпульсній заваді безперешкодно досягати чутливих входів цифрових мікросхем, перевантажувати їхні внутрішні кола захисту та безпосередньо впливати на логічні стани транзисторів.

Метою сучасних імпульсних атак рідко є фізичне знищення апаратури, натомість більшу загрозу для систем кібербезпеки та криптографічних модулів становлять недеструктивні впливи, що призводять до виникнення так званих «м'яких помилок» (soft errors) або тимчасових логічних збоїв [6].

Найкритичнішим для безпеки мікроконтролерних систем є наведення завад на такі схемотехнічні вузли:

– лінії тактування (Clock Lines) та системи фазового автопідлаштування частоти (PLL). Інжекція високочастотного імпульсу в коло кварцового резонатора або тактову шину спричиняє раптову зміну тривалості такту або генерацію хибного фронту сигналу. У результаті процесорне ядро втрачає синхронізацію з пам'яттю, що призводить до пропуску виконання окремих машинних інструкцій. У криптографії це дозволяє зловмиснику пропустити команду перевірки пароля або порушити цикл розгортання ключа шифрування;

– шини даних та управління. Електромагнітна наводка, що збігається в часі з моментом зчитування даних, здатна викликати миттєву інверсію логічного стану окремого біта. Передача спотвореного біта по шині даних може повністю змінити хід виконання програми або призвести до витоку інформації через алгоритми диференціального криптоаналізу [6];

– кола живлення та лінії скидання. Високоенергетичні імпульси здатні викликати короткочасні просадки напруги або різкі сплески на шині живлення мікроконтролера. Такі коливання напруги часто призводять до хибного спрацьовування супервізора живлення, ініціюючи несанкціоноване перезавантаження пристрою.

Таким чином, електромагнітний імпульс діє як безконтактний інструмент внесення несправностей, що дозволяє маніпулювати станом цифрової схеми без фізичного втручання в її топологію.

Оскільки програмні методи захисту (такі як криптографічні алгоритми або сторожові таймери) виявляються неефективними проти атак на фізичному рівні, головна роль у забезпеченні стійкості припадає схемотехнічному проектуванню та конструюванню друкованих плат (PCB).

Виходячи з аналізу сучасних методів забезпечення EMC, ключовим підходом до захисту від навмисних електромагнітних імпульсів (IEMI) є багаторівневе екранування та апаратна фільтрація:

– PCB Layout (топологія друкованої плати). Використання багатошарових плат із Ground Planes (суцільними полігонами заземлення) та живлення є базовою вимогою. Це створює розподілену паразитну ємність, яка поглинає високочастотні сплески, та мінімізує площу контурів протікання струму. Це критично важливо для зниження індуктивності петлевих антен, які приймають електромагнітну заваду [5];

– PCB Shielding (локальне екранування). Встановлення металевих екранів безпосередньо над критично важливими компонентами, такими як мікроконтролери, модулі пам'яті та радіочастотні тракти. Екран функціонує як клітка Фарадея, відбиваючи та поглинаючи енергію зовнішнього надширокосмугового електромагнітного поля. При цьому найважливішою умовою є забезпечення безперервного електричного контакту екрана з полігоном заземлення плати по всьому периметру для надшвидкого та ефективного відведення наведених струмів [5];

– компонентний захист та фільтрація. Для захисту кіл введення-виведення та шин живлення, що

неминуче виходять за межі локальних екранів, застосовуються напівпровідникові обмежувачі напруги – швидкодіючі TVS-діоди (Transient Voltage Suppressors). Вони здатні за наносекунди зрізати високовольтні піки, параметри яких регламентовані стандартом ДСТУ IEC 61000-4-2 [4]. Крім того, для ліній передачі даних ефективним рішенням є перехід на диференційну передачу сигналів, що дозволяє на апаратному рівні компенсувати синфазні завади, індуковані електромагнітним імпульсом [2].

Таким чином, аналіз розглянутих методів апаратного захисту свідчить про те, що жодне з наведених схемотехнічних рішень не здатне самостійно забезпечити абсолютну стійкість електронної апаратури до потужних електромагнітних імпульсних атак. Лише комплексне застосування топологічних методів трасування, просторового екранування критичних вузлів та інтеграції швидкодіючої захисної компонентної бази дозволяє створити ешелоновану систему захисту.

Висновки

У роботі проаналізовано проблематику вразливості сучасних цифрових систем та апаратних засобів криптографічного захисту інформації до навмисних електромагнітних імпульсних атак (IEMI). В умовах безперервної мініатюризації компонентної бази та зниження номінальних напруг живлення, мікроелектроніка втрачає природний запас завадостійкості. У результаті навіть наносекундні надширокосмугові імпульси здатні індукувати паразитну ЕРС, яка викликає критичні апаратні збої: «м'які помилки» (інверсію бітів у шинах даних), фазове тремтіння тактових генераторів та хибне спрацьовування кіл скидання. Традиційні програмні механізми кібербезпеки є абсолютно неефективними проти таких атак, оскільки високоенергетичний імпульс діє на фізичному рівні, в обхід операційної системи, безпосередньо маніпулюючи станом логічних вентилів процесора.

Для надійного захисту інформаційних систем необхідно створити ешелоновану систему апаратної безпеки, яка має закладатися ще на ранніх етапах схемотехнічного та топологічного проектування. Лише комплексне поєднання пасивних конструктивних методів (суворе дотримання правил трасування багатошарових друкованих плат, використання суцільних полігонів заземлення для мінімізації площі приймальних контурів, локальне екранування критичних мікросхем) та швидкісної компонентної фільтрації (застосування TVS-діодів та диференційних ліній зв'язку) здатне забезпечити необхідний рівень стійкості.

Виконання вимог чинних нормативних стандартів електромагнітної сумісності (зокрема, ДСТУ IEC 61000-4-2) та впровадження комплексного апаратного захисту є критично необхідними умовами для гарантування безперебійної та безпечної роботи систем критичної інфраструктури, IoT-пристроїв та спеціальної електроніки в умовах сучасних кіберфізичних загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стандарт EMC і сертифікація. URL: https://pneumatyka.com.ua/p/standart-emc-i-sertifikaciya (дата звернення: 21.03.2026).
2. Лазебний В. С., Пілінський В. В., Швайченко В. Б. Електромагнітна сумісність електронних засобів. [Навчальний посібник]. – Київ: КПІ ім. Ігоря Сікорського, 2023. (дата звернення: 22.03.2026).
3. Плугін В. Є., Плугіна О. А. Конспект лекцій з дисципліни «Електромагнітна сумісність у системах електроспоживання». URL:https://eprints.kname.edu.ua/48989/1/2018%20%D0%BF%D0%B5%D1%87.%20134%D0%9B%20%D0%9A%D0%9E%D0%9D%D0%A1%D0%9F%D0%95%D0%9A%D0%A2%20%D0%95%D0%9C%D0%A1.doc.pdf (дата звернення 24.03.2026).
4. ДСТУ IEC 61000-4-2:2008. Електромагнітна сумісність. Частина 4-2. Методи випробування та вимірювання. Випробування на несприйнятливість до електростатичних розрядів. URL: https://vtechworks.lib.vt.edu/server/api/core/bitstreams/5e7802ec-ed7c-43de-8f93-23460a50df74/content (дата звернення: 24.03.2026).
5. Методи екранування друкованих плат для контролю електромагнітних перешкод і відповідності стандартам електромагнітної сумісності. [Електронний ресурс]. – URL: https://hilelectronic.com/uk/pcb-shielding/ (дата звернення 27.03.2026).
6. Electromagnetic Interference Attacks on Cyber–Physical Systems: Theory, Demonstration, and Defense. [Електронний ресурс]. – URL: https://vtechworks.lib.vt.edu/server/api/core/bitstreams/5e7802ec-ed7c-43de-8f93-23460a50df74/content (дата звернення 01.04.2026).

Крістіна Вікторівна Пугачева – студентка групи 2КІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: kristipref@gmail.com

Науковий керівник: ***Бондаренко Ірина Олексіївна –*** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Puhacheva Kristina V. – student of group 2KITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: kristopref@gmail.com

Supervisor: ***Bondarenko Iryna O.*** **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua