Науково-дослідна частина
Національного університету
кораблебудування
імені адмірала Макарова

54025, м. Миколаїв,
пр. Героїв України, 9
Тел.: (0512) 70-91-04
http://conference.nuos.edu.ua
e-mail: conference@nuos.edu.ua

Навчально-науковий інститут
автоматики та електротехніки
Національного університету
кораблебудування
імені адмірала Макарова

54021, м. Миколаїв,
пр. Центральний, 3
Тел.: (0512) 47-70-95
http://iae.nuos.edu.ua
e-mail: university@nuos.edu.ua

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

НАУКОВО-ТЕХНІЧНІ КОНФЕРЕНЦІЇ
Національний університет кораблебудування
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

МАТЕРІАЛИ

XI ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

23-24 листопада 2023 р.

Миколаїв ■ НУК ■ 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2023

МАТЕРІАЛИ

XI Всеукраїнської науково-технічної конференції з міжнародною участю

23–24 листопада 2023 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2023

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Матеріали публікуються за оригіналами, наданими авторами.
Претензії до організаторів не приймаються.

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2023. – 223 с.

У збірнику подано матеріали XI Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, системи Інтернет речей (IoT), моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

УДК 621.318; 004.056

ЕЛЕКТРОМАГНІТНА СУМІСНІСТЬ ЯК ВПЛИВОВИЙ ФАКТОР РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автор: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

На перших етапах розвитку теорії електромагнітної сумісності (ЕМС) більшість наукових робіт була пов'язана із ЕМС радіообладнання. Зокрема, науковці і практики намагалися вирішити питання шумів, завад і заземлення для забезпечення якісного радіозв'язку.

На даний час проблема ЕМС розглядається у глобальному масштабі, і її вирішенню присвячена діяльність:

– міжнародних, регіональних і національних організацій із стандартизації, що має на меті гарантувати якість товарів і послуг на міжнародному ринку [1-4];

– науковців, виробників товарів і постачальників послуг, спрямована на вирішення питань ЕМС на теоретичному і практичному рівнях для певних пристроїв, установок, технологій і галузей, які характеризуються різними діапазонами робочих частот і потужностей, працюють в різній електромагнітній обстановці (ЕМО), мають різний рівень імунітету (несприйнятливості) до відхилень ЕМО від нормованих значень і є джерелами емісії в різних діапазонах частот і потужностей [5-10].

Збої, викликані порушенням ЕМС, можуть впливати на порушення штатних режимів роботи засобів обробки інформації і засобів захисту інформації.

Метою даної роботи є визначення впливу порушення ЕМС на ризики інформаційної безпеки.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– визначити фактори, що негативно впливають на ЕМС комп'ютерних систем (КС);

– визначити наслідки порушення ЕМС з точки зору ризиків інформаційної безпеки.

Широке впровадження інформаційних технологій у всі сфери людської діяльності і побуту, поширення автоматизованих систем у технологіях виробництва різноманітних товарів, розповсюдження побутових електричних приладів суттєво ускладнюють електромагнітну обстановку для будь-якого сучасного електрообладнання.

Крім того, проблема ЕМС загострюється внаслідок наявних трендів у галузі електроніки [9], що є елементною базою пристроїв обробки та захисту інформації:

– наявна тенденція до зниження рівнів порогових напруг елементної бази. Перехід від технологій реалізації перетворювальних пристроїв і засобів обробки сигналів на електронних вентилях, порогові напруги для яких могли сягати до кількох сотень вольт, до сучасної цифрової логіки і мікросхемо техніки, порогові напруги яких складають кілька вольт, підвищує чутливість сучасної елементної бази електронних пристроїв до впливу сторонніх електромагнітних полів (ЕМП), тобто знижує імунітет обладнання;

– наявна тенденція до пришвидшення процесів обробки та передавання сигналів, зумовлена необхідністю обробляти постійно зростаючі в інформаційному суспільстві обсяги інформації, ускладненням автоматизованих систем (АС) та систем керування ними. Для досягнення високих швидкостей обробки сигналів в електронних блоках обладнання застосовують схемо технічні рішення, які забезпечують коротші імпульси з крутими фронтами наростання і спадання. Зменшення часу наростання імпульсу призводить до того, що зростає доля енергії, яка перетворюється на високих частотах внаслідок появи високочастотних гармонік. Електромагнітні випромінювання високої частоти здатні поширюватися на великі відстані і, відповідно, негативно впливати на ЕМО як на місці експлуатації електрообладнання, так і на віддалених територіях;

– наявна тенденція до використання при виробництві електрообладнання не провідникових матеріалів для корпусів обладнання і/або його окремих блоків, наприклад, пластмаси. Такі матеріали є більш дешевими, однак вони не мають таких екрануючих властивостей як металевий корпус, внаслідок чого погіршується ЕМО на місці експлуатації обладнання. ЕМО на віддалених територіях також може погір-

шуватися, що залежить не тільки від наявних екранів, а й від частот електромагнітних випромінювань певного обладнання;

– наявна тенденція до мініатюризації напівпровідникових приладів і мікросхем, застосування планарних конструкцій також негативно впливає на ЕМО для цих компонентів електрообладнання, внаслідок зменшення відстаней, на які вони рознесені, підвищення щільності локальних енергетичних впливів і погіршення умов охолодження приладів, що викликає появу додаткових теплових шумів і гармонік, значимих струмів витоку.

Негативний вплив на ЕМС обладнання також має тенденція до викривлення напруги його живлення, яка зумовлена:

– сезонними і добовими коливаннями споживаної потужності в електричній мережі, вмиканням та вимиканням потужних споживачів, які спричиняють зниження, провали, відключення і підвищення напруги і, як наслідок, відключення, перевантаження та вихід з ладу обладнання, що змінює ЕМО;

– атмосферними явищами (грозовими розрядами), які можуть викликати появу високовольтних імпульсів і супроводжуються генерацією високочастотних коливань;

– взаємним впливом електрообладнання, розташованого на одній території, що викликає появу електричних шумів;

– процесами в установках і обладнанні споживачів, пов'язаними з генерацією в мережу гармонік, що викривлюють форму кривої споживаної потужності, і реактивної потужності, що змінює енергетичний баланс;

– застосуванням імпульсних джерел вторинного електроживлення в комп'ютерних мережах і системах, автоматизованих системах тощо. Джерела вторинного електроживлення ключового типу на даний час є одними з найбільш розповсюджених джерел електромагнітних завад, і спричиняють зростання рівнів і розширення спектрів завад, тобто змінюють гармонійний склад напруги живлення та ЕМО як на місці експлуатації джерел вторинного електроживлення і систем, для яких вони призначені, так і на територіях, віддалених на відносно невелику відстань, що зумовлено процесами згасанням;

– застосуванням електричної мережі як середовища передачі сигналів.

Перелічені вище впливові фактори призводять до зростання рівнів і розширення спектрів завад у системах електроживлення обладнання і ускладнення електромагнітної обстановки.

Порушення ЕМС може викликати збої в роботі в роботі пристроїв обробки та захисту інформації, тобто є джерелом загроз інформаційної безпеки (ІБ). Загрози ІБ можуть бути класифіковані за різними критеріями, зокрема, згідно НД ТЗІ 2.5-004-99 [11] комплекс засобів захисту повинен надавати послуги:

– із захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Порушення ЕМС апаратних і апаратно-програмних засобів розмежування доступу може привести до тимчасової або остаточної втрати працездатності таких засобів і, відповідно, до порушення конфіденційності інформації;

– із захисту оброблюваної інформації від несанкціонованої модифікації. Порушення ЕМС апаратно-програмних складових обробки інформації в процесі запису і видалення інформації може привести до порушення цілісності інформації;

– із забезпечення доступності інформаційниї ресурсів та послуг на певному проміжку часу і спроможності КС відновлюватися і функціонувати в разі відмови її компонентів. Порушення ЕМС безпосередньо впливає на стійкість до відмов і відновлення обладнання після збоїв;

– із забезпечення спостереженості як засобу підтримки спроможності КЗЗ виконувати свої функції. Порушення ЕМС може вплинути на індикатори процесів і результати само тестування.

Крім того, згідно НД ТЗІ 2.5-004-99 [11] для гарантування коректності реалізації КЗЗ для рівнів гарантій вище третього мають бути наявні методики забезпечення фізичної і технічної безпеки, в яких за змістом потрібно враховувати ЕМО, побічні випромінювання і наведення тощо, тобто приймати до уваги параметри ЕМС обладнання.

Таким чином, порушення ЕМС може бути джерелом загроз і, відповідно, ризиків порушення конфіденційності, цілісності і доступності інформації.

При керуванні ризиками інформаційної безпеки [12] загрози за ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) [13] класифікуються за іншими критеріями: за природою виникнення, за типом наслідків загроз і за типами зловмисників.

За природою виникнення порушення ЕМС може бути класифіковане як:

– навмисна загроза (категорія *D*), граничним випадком якої є застосування зловмисником електромагнітної зброї або засобів радіоелектронної боротьби;

– випадкова загроза (категорія *A*), якщо внаслідок випадкових, ненавмисних дій людини порушення ЕМС негативно впливає на інформаційні активи;

– природна (екологічна) загроза (категорія *E*), якщо порушення ЕМС відбувається внаслідок природних причин, які не пов'язані із цілеспрямованими або випадковими діями людини, наприклад, внаслідок деградаційних процесів в обладнанні, внаслідок грозових розрядів тощо.

За типом наслідків загроз порушення ЕМС може бути класифіковане як:

а) фізичні пошкодження категорій *A, D, E*, якщо відхилення параметрів ЕМС є суттєвим і спричиняє вихід обладнання з ладу;

б) природна подія (категорія *E*), якщо порушення ЕМС є наслідком грозових розрядів;

в) втрата необхідних сервісів, якщо порушення ЕМС спричиняє: відмову телекомунікаційного обладнання або сервісних систем АС, наприклад, системи охолодження, (категорії *A, D*) або втрату електроживлення (категорії *A, D, E*);

г) несправність внаслідок негативного впливу випромінювання різної природи: теплового, електромагнітного, радіаційного випромінювання, електромагнітних імпульсів (категорії *A, D, E*);

д) компрометація інформації категорії *D*, якщо порушення ЕМС пов'язане з перехопленням і відправленням скомпрометованого сигналу, дистанційним шпигуванням, виявленням місця розташування або втручанням в роботу апаратних і програмних засобів;

е) технічна відмова категорії *A*, якщо наслідком порушення ЕМС є відмови і збої в роботі апаратно-програмних засобів, або категорій *A, D*, якщо наслідком є втрата ремонтопридатності АС;

ж) несанкціонована дія категорії *D*, якщо порушення ЕМС пов'язане з несанкціонованим використанням обладнання, викривленням даних, несанкціонованою обробкою даних;

з) компрометація функцій категорії *A*, якшо порушення ЕМС спричиняє помилки у використанні, або категорій *A, D, E,* якщо наслідком порушення ЕМС є порушення працездатності персоналу. В останньому випадку мають прийматися до уваги Державні санітарні норми і правила [14].

За типами зловмисників порушення ЕМС може бути класифіковане як:

– загроза, викликана діяльністю комп'ютерних злочинців, якщо для реалізації порушення ЕМС АС використовувалася комп'ютерна техніка;

– промислове шпигунство, якщо порушення ЕМС було здійснене в інтересах конкурентів або в інтересах певних урядових груп (в тому числі іноземних);

– загроза створена інсайдерами (співробітниками недостатньої кваліфікації; невдоволеними, зловмисними або недбалими співробітниками).

Висновки

В даній роботі проведено аналіз проблеми ЕМС і визначені фактори, що негативно впливають на ЕМС комп'ютерних систем, та наслідки порушення ЕМС з точки зору ризиків інформаційної безпеки. Показано, що порушення ЕМС може бути класифіковане як загроза інформаційної безпеки і може непрямим чином викликати порушення конфіденційності, цілісності і спостереженості інформації та безпосередньо впливати на доступність інформації. Наявні тренди в динаміці факторів, які негативно впливають на ЕМС КС, дозволяють стверджувати, що ризики інформаційної безпеки внаслідок порушення ЕМС надалі зростатимуть.

Список літератури:

1. Committed to connecting the world. About International Telecommunication Union (ITU). URL: https://www.itu.int/en/about/Pages/default.aspx

2. Committed to connecting the world. TIES Services. URL: https://www.itu.int/en/ties-services/Pages/default.aspx

3. ITU-R SM.329-10. Unwanted emissions in the spurious domain. URL: https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.329-10-200302-S!!PDF-E.pdf

4. Перелік національних стандартів для цілей застосування Технічного регламенту з електромагнітної сумісності обладнання, затвердженого постановою Кабінету Міністрів України від 16.12.2015 № 1077, затверджений Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України 08 грудня 2020 року № 2569. URL: https://zakon.rada.gov.ua/rada/show/v2569915-20#n11

5. Keller R.B Design for Electromagnetic Compatibility–In a Nutshell Theory and Practice (eBook). Open access publication. – Switzerland, Cham: Springer, 2023. – 423 p. URL: https://library.oapen.org/bitstream/id/46a00bde-bd59-42f6-a21f-072289004fa3/978-3-031-14186-7.pdf

6. Дакі О.А., Іваненко В.М., Федунов В.М., Бажак О.В. Електромагнітна сумісність систем зв'язку та оповіщення у надзвичайних ситуаціях на морі // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2021. – №2(68). – С.38-44. URL: https://journal-hnups.com.ua/index.php/zhups/article/view/593/506

7. Електромагнітна зброя: Від потенціалу до реалізації – ключ до підвищення обороноздатності України. URL: https://zovu.org/elektromagnitnoye-oruzhiye-ot-potentsial/

8. Король Е.Г., Пантелят М.Г. Требования по электромагнитной совместимости технических средств на объектах электроэнергетики и промышленности // Вісник НТУ "ХПІ". – 2013. – No15 (988). – С.35-60. URL: http://pema.khpi.edu.ua/article/view/13170/11060/

9. Лазебний В.С., Пілінський В.В., Швайченко В.Б. Електромагнітна сумісність електронних засобів: Навчальний посібник. Електронне мережне навчальне видання. – К.: КПІ ім. Ігоря Сікорського, 2023. – 343 с.

10. Розорінов Г.М., Платоненко А.В. Захист інформаційних систем від потужних електромагнітних випромінювань //Сучасний захист

інформації. – 2014. – №3. – С.16-20. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/180/178

11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342

12. Корченко О.Г., Гнатюк С.О, Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навчально.-наукових. та науково-практичних видань НА СБ України, 2014. – 190 с.

13. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. URL: https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400

14. ДСанПіН № 3.3.6.096-2002 Державні санітарні норми і правила при роботі з джерелами електромагнітних полів, затверджені наказом Міністерства охорони здоров'я України від 18 грудня 2002 року № 476, зареєстрованих в Міністерстві юстиції України 13 березня 2003 року за № 203/7524. URL: https://zakon.rada.gov.ua/laws/show/z0203-03

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2023

XI Всеукраїнська науково-технічна конференція
з міжнародною участю

23–24 листопада 2023 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською мовою*)

Відповідальна за випуск В. В. Трибулькевич