УДК 004.056

Г.М. Розорінов, А.В. Платоненко

ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД ПОТУЖНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ

Розглянуто проблему захисту інформаційних систем від навмисного потужного електромагнітного впливу. На основі отриманих даних показано, що характер порушень в роботі електронного устаткування безпосередньо залежить від параметрів і рівня стійкості устаткування до електромагнітного впливу. Дано систематизований перелік можливих наслідків для засобів інформатизації, використовуваних в основних сферах діяльності.

Ключові слова: безпека, генератор, потужний електромагнітний вплив, захист інформаційних систем.

Вступ

Ефективність і безпека роботи різноманітних науково-виробничих комплексів (НВК) багато в чому досягається завдяки застосуванню засобів інформатизації в різних сферах їх діяльності. Основну загрозу для інформаційних ресурсів до недавнього часу представляли хакерські атаки і впровадження комп'ютерних вірусів, які здійснюються програмним шляхом. Проте створення компактних генераторів потужних електромагнітних випромінювань, здатних негативно впливати на електронне устаткування, істотно змінило пріоритети в області інформаційної безпеки [1]. Сьогодні, в розряд першочергових, висувається проблема захисту від навмисного електромагнітного впливу [2].

Основна частина

Дослідження в області дії потужних електромагнітних випромінювань на електронну інфраструктуру і пошук захисту від них активно ведуться в різних країнах. Джерела електромагнітних імпульсів розробляються в ряді країн з метою досягнення якісно нового рівня радіолокації, радіозв'язку, технологій вирішення інших технічних завдань. Принцип їх роботи допускає генерацію і випромінювання в навколишній простір не лише одиничних електромагнітних сигналів, але і цілих пакетів. Параметри випромінювання таких пристроїв роблять їх дуже небезпечними при дії на мікроелектронні системи. Відносна простота виготовлення і доступність придбання таких генераторів, а також компактність цих приладів дозволяють розцінювати їх в якості потенційних засобів навмисного впливу, що дозволяють локально створювати ефекти, подібні до електромагнітних випромінювань ядерного вибуху.

Існує широка номенклатура генераторів, що формують електромагнітні імпульси, які призначені для перевірки стійкості електронного устаткування різних об'єктів до електромагнітного впливу. Характер порушень в роботі безпосередньо залежить від параметрів і рівня стійкості устаткування до цього впливу. Порушення в основному носять тимчасовий характер, проявляються під час впливу і зберігаються впродовж деякого періоду після цього впливу, причому виявити факт навмисного електромагнітного впливу, як в цей період, так і надалі – є не можливим.

Електронна інфраструктура НВК, ставши об'єктом електромагнітної атаки, може зазнати ряд деструктивних змін, що, у свою чергу, приведе до збоїв в роботі електронного устаткування і далі – до функціональних порушень видів діяльності, що ним забезпечується.

Систематизований перелік можливих наслідків для засобів інформатизації, використовуваних в основних сферах діяльності, властивих об'єктам НВК, приведений в табл. 1.

Таблиця 1

Деструктивні ефекти в електронному устаткуванні
при навмисному електромагнітному впливі (НЕМВ)

Вид системи	**Вид ефекту в результаті дії**
Засоби телекомунікації	- зависання і перезавантаження комп'ютерів, - значне зниження інформаційного трафіку, - збільшення кількості помилок.
Засоби зв'язку і навігації	- зменшення ефективної дальності зв'язку (від 2 до 10 разів), - неправдиві свідчення, або збої в засобах навігації.
Засоби безпеки	- збої в системах контролю і управління доступом, - блокування охоронно-пожежної сигналізації, - мимовільне включення устаткування пожежогасіння, - спотворення зображень з камер відео нагляду.

Варто відмітити, що збиток від електромагнітного нападу може бути порівняний з наслідками прямих терористичних атак (рис. 1).

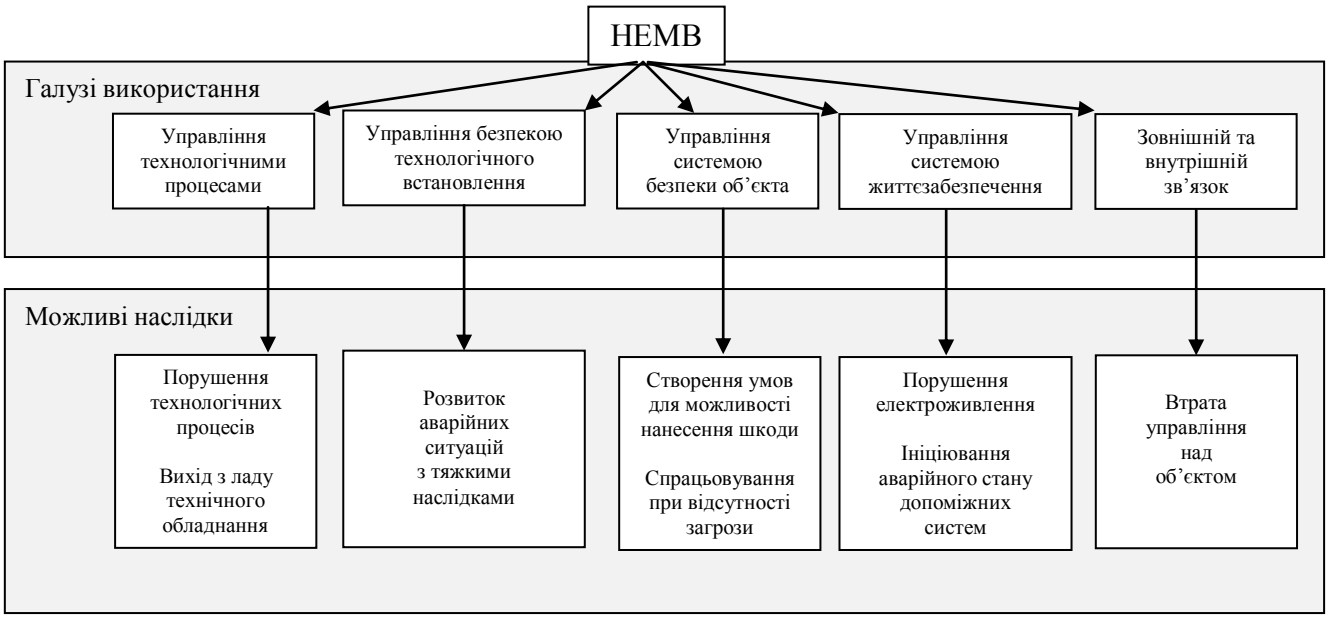

Рис.1. Галузі використання інформаційних систем та можливі наслідки НЕМВ

Проблему захисту інформаційних систем від навмисного електромагнітного впливу намагаються розв'язати фахівці різних країн.

Основним напрямом міжнародної діяльності є розробка цільових стандартів по забезпеченню стійкості цивільних об'єктів до впливу потужних електромагнітних випромінювань. В їхньому числі – методи оцінки стійкості до таких впливів на інформаційні системи телекомунікаційної апаратури і центрів обробки даних, практичні методи захисту комп'ютерних систем, тощо.

Міра ушкодження системи залежить від стійкості як кожного з компонентів пристроїв, так і від енергії потужної завади в цілому, яка може бути поглинена схемою без виявлення дефекту або відмови.

Наприклад, для електромагнітного реле з котушкою на напругу 230 В змінного струму комутаційна завада від індуктивного навантаження з амплітудою 500 В, хоча і є більш ніж двократним перенапруженням, але навряд чи приведе до відмови реле в силу стійкості електромеханіки до такого роду завад, та в свою чергу, малої тривалості такої завади (впродовж мікросекунд). Інакше виходить з мікросхемою, що живиться від джерела 5 В постійного струму. Імпульсна завада з амплітудою 500 В, у 100 разів перевищує напругу живлення цього електронного компонента і призводить до неминучої відмови і подальшого руйнування пристрою. Стійкість мікросхем до перенапружень на декілька порядків нижче, ніж стійкість електромагнітного реле [2, 3].

Оскільки завади, що мають меншу енергію, виникають частіше ніж завади, що мають велику енергію, найбільш частою реакцією електронних систем на дію електромагнітних завад буде не руйнування пристрою, а порушення його роботи або короткочасний збій в роботі з наступним відновленням порушеної функції (рис. 2).

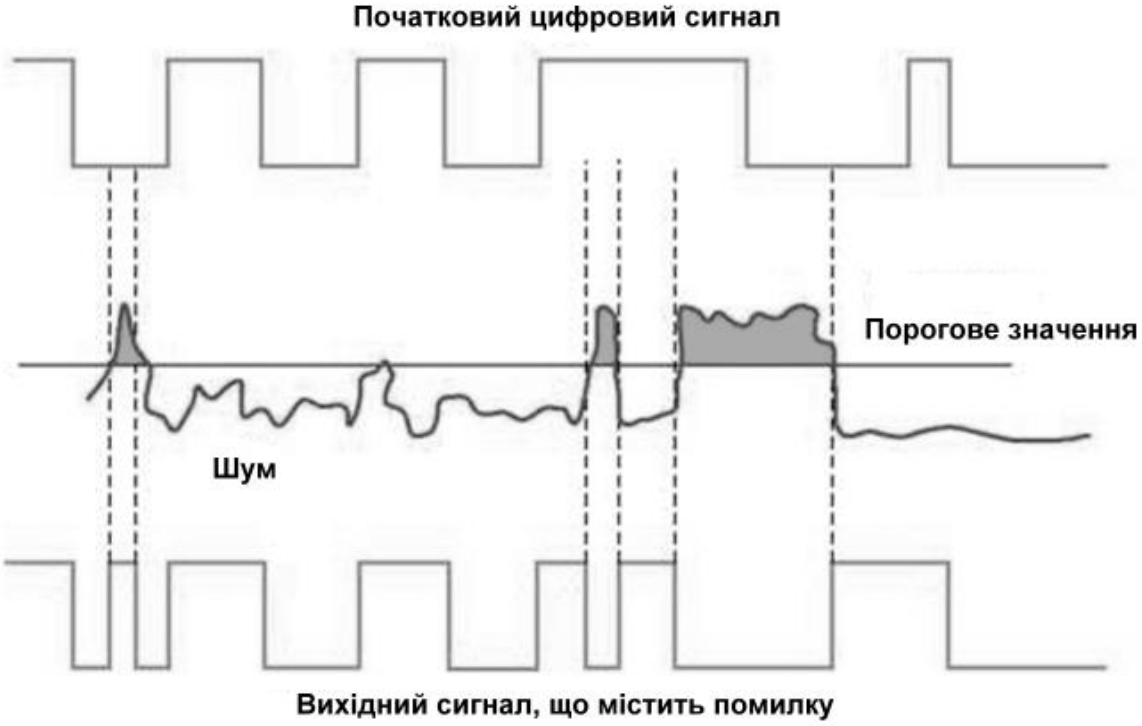

Рис. 2. Вплив завади малої енергії на роботу цифрового приладу

Імпульсні перенапруження, що виникають при розрядах блискавок і при комутації в силових електроустановках, здатні пошкодити, або зруйнувати як електронні прилади, так і цілі системи. Кожну секунду близько 50 блискавок вдаряють по поверхні землі, і в середньому кожен її квадратний кілометр блискавка вражає шість разів за рік. Напруга блискавки може складати до ста мільйонів вольт. У нормах будівництва громовідводів приймають зазвичай струм блискавки до 200 тисяч ампер при тривалості близько 1 мс, хоча практично струм блискавки рідко перевищує 20-30 кА. Температура каналу при головному розряді може перевищувати 25000^{o} С. Довжина каналу блискавки може бути від 1 до 10 км, діаметр — декілька сантиметрів. При ударі блискавки в громовідвід електричний струм (у вигляді імпульсу дзвоноподібної форми, рис. 3) поступає в землю і розтікається в грунті на всі боки до декількох десятків і навіть сотень метрів, причому із-за опору грунту цей струм створює на ньому падіння напруги. Оскільки найбільший опір чинять шари грунту, що лежать поблизу місця входження струму в землю, то саме тут спостерігається найвища напруга. В міру видалення від цієї точки опір проходженню струму зменшується, при цьому знижується і напруга (рис. 3).

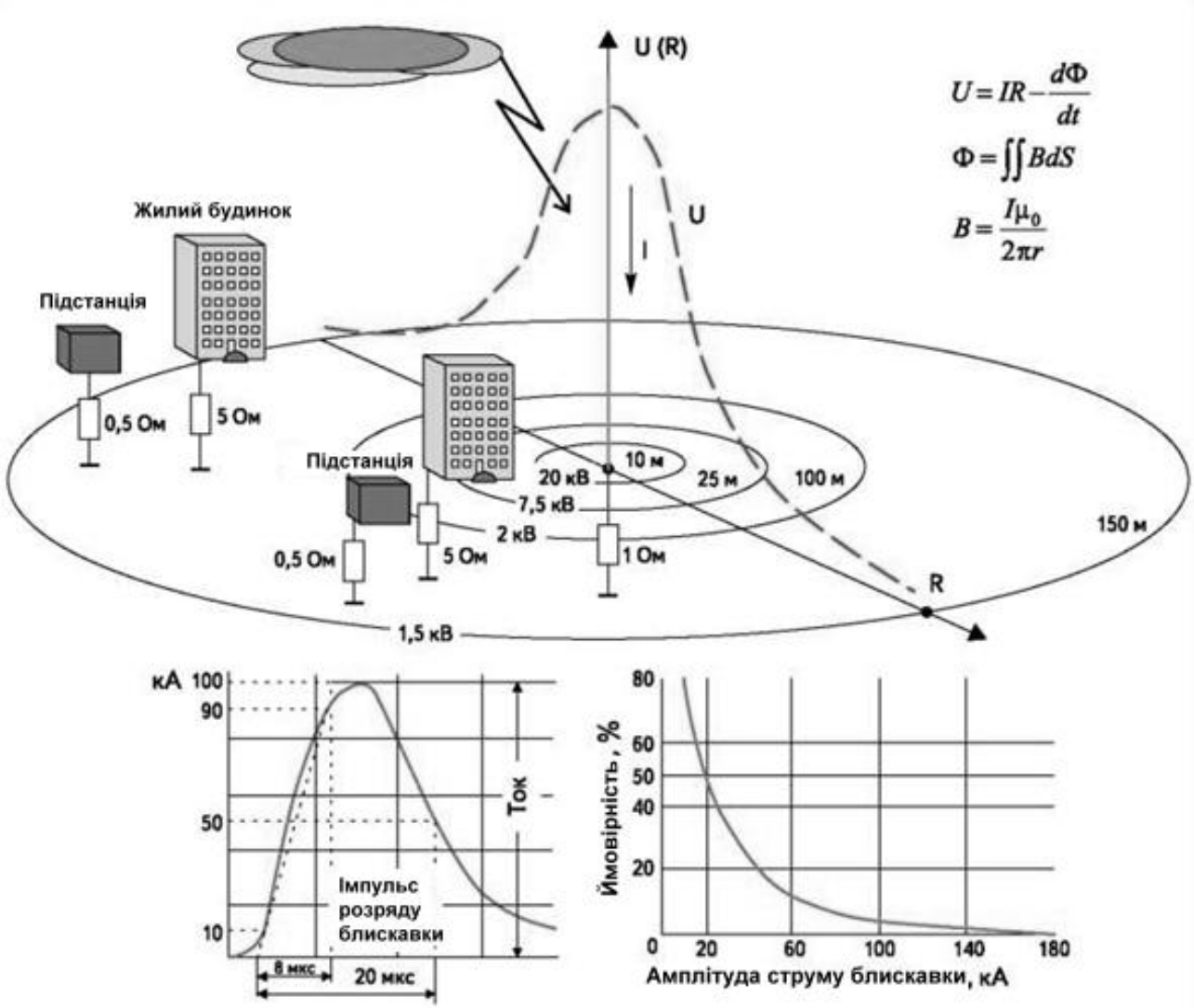

Рис.3. Процеси, що відбуваються при попаданні блискавки у громовідвід

Для зниження потенціалу, що наводиться при протіканні струму блискавки в грунті, опір розтіканню струму в зоні розташування житлових і промислових будівель і споруд зменшують за допомогою металевої сітки досить великої площі, розміщеної в грунті під фундаментом будівель. Проте опір таких заземляючих систем все ще дуже далеко від нуля (рис. 3), і тому навіть залишкові імпульсні потенціали, наведені в заземляючій системі і проникаючі по кабелях на входи електронної апаратури, представляють для неї серйозну небезпеку. Завади такого роду називаються кондуктивними. Окрім завад такого виду, імпульс сильного струму, що проходить по громовідводу, створює і завади у вигляді електромагнітних полів, що впливають на усі близько розташовані провідники. Така дія називається індуктивною.

Існують ще і ємнісні наведення, при яких короткі (тобто високочастотні) імпульси перенапруження з високовольтних ліній електропередач потрапляють в низьковольтні ланцюги через ємнісні зв'язки між обмотками трансформаторів.

В процесі поширення завади, має місце багатократне перетворення одного виду на інший, тому таке ділення дуже умовне, особливе коли йдеться про високочастотні процеси. (Імпульс розрядного струму блискавки з досить крутими фронтами — 8 і 20 мкс (рис. 3) — можна розглядати саме як такий високочастотний процес.) Тому аналіз розтікання струму в землі через заземляючі пристрої вимагає обліку обох цих складових. Більше того,

потрапивши в електронну апаратуру за допомогою електромагнітного поля або по дротах, завада зазнає численні перетворення вже всередині цієї апаратури із-за наявності паразитних ємнісних і індуктивних зв'язків між окремими елементами, або між різними вузлами апаратури. При цьому високочастотна складова завади може проникати углиб апаратури, в обхід встановлених фільтрів і захисних елементів [4-6].

Ще один шлях для проникнення завади від розряду блискавки — протікання струмів по заземленому металевому корпусу і заземленим екранам численних кабелів, підключених до нього. Усе це говорить про те, що забезпечити належний рівень захисту від електромагнітних завад електронної апаратури дуже і дуже непросто. Особливо складно це зробити на старих підстанціях, системи заземлення яких проектувалися для роботи з електромеханічним захистом, значно стійкішим до електромагнітних дій, чим мікропроцесорна. А якщо врахувати, що небезпечні підйоми потенціалу в ланцюгах заземлення виникають не лише при ударах блискавки, але і при аварійних коротких замиканнях в електричних мережах, то проблема стане ще складнішою.

В деяких випадках для запобігання такому підйому потенціалу в ланцюгах електронної апаратури контури заземлення силового устаткування і електронної апаратури роблять роздільними. Проте на реально існуючих підстанціях виконати таке розділення нереально.

На нашу думку, тільки комплексне рішення проблеми дозволить уникнути впливу потужних електромагнітних завад. Це рішення повинне включати:

- використання мікропроцесорних реле захисту тільки на підстанціях, спроектованих і побудованих з урахуванням найсучасніших вимог до електромагнітної сумісності і розрахованих на експлуатацію високочутливої електронної апаратури;
- вдосконалення конструкції самих мікропроцесорних реле захисту;
- розміщення мікропроцесорних реле захисту в металевих шафах, спеціально призначених для захисту електронного устаткування і забезпечених фільтрами на усіх кабелях, що входять в шафу.

Висновки

Зафіксовано електромагнітні атаки на системи безпеки і комп'ютерні мережі банків, автомобільні системи безпеки, військові системи радіозв'язку. З метою забезпечення безпеки об'єктів НВК, необхідно створювати для них системи захисту інформації від несанкціонованого доступу, знищення, модифікації та блокування інформації. Це передбачає планування і реалізацію комплексу технічних і організаційних заходів, що забезпечують захищеність об'єктів НВК.

Література

1. Кузнєцов М., Кунгуров Д., Матвєєв М., Тарасов В. Вхідні ланцюги облаштувань РЗА. Проблеми захисту від потужних імпульсних перенапружень. Новини електротехніки. 2006. - 6 с

2. Іванов П. Trabtech — технологія для захисту електроустаткування від імпульсних перенавантажень. Компоненти і технології. 2003. - 7 с.

3. Борисов Р. Невнимание к проблеме ЭМС может обернуться катастрофой // Новости электротехники. 2001. № 6 (12). – 10 с.

4. Matsumoto T., Kurosawa Y., Usui M., Yamashita K., Tanaka T. Experience of Numerical Protective Relays Operating in an Environment with High-Frequency Switching Surge in Japan // IEEE Transactions On Power Delivery. Vol. 21. No. 1. 2006. – 21 c.

5. Carsimanovic S., Bajramovic Z., Ljevak M., Veledar M., Halilhodzik N. Current Switching with High Voltage Air Disconnector // International Conference on Power Systems Transients (IPST'05). Montreal, Canada. 19-23 June, 2005. - 35 c.

6. Mohana Rao M., Joy Thomas M., Singh B. P. Transients Induced on Control Cables and Secondary Circuit of Instrument Transformers in a GIS During Switching Operations // IEEE Trans. on Power Delivery. Vol. 22. No. 3. July, 2007. – 15 c.

Надійшла 23.07.2014 р. Рецензент: д.т.н., проф. Толюпа С.В.