УДК 004.73:621.391.8
DOI: 10.31673/2412-9070.2023.022124

Л. П. КРЮЧКОВА, доктор техн. наук, професор;
Д. О. ТАРАСЕНКО, аспірант,
Державний університет телекомунікацій, Київ

ІНФОКОМУНІКАЦІЙНІ МЕРЕЖІ ЯК ОБ'ЄКТ НАВМИСНИХ ДЕСТРУКТИВНИХ ЕЛЕКТРОМАГНІТНИХ ВПЛИВІВ

Навмисні деструктивні електромагнітні впливи, сформовані на основі наявних технічних засобів, є ефективним видом сучасних радіоелектронних інформаційно-технічних впливів на інфокомунікаційні мережі. Мета публікації — розгляд уразливостей сучасних інфокомунікаційних мереж від навмисних деструктивних електромагнітних впливів, під якими розуміють навмисне створення в злочинних або терористичних цілях потужного електромагнітного впливу на електронні та електричні системи для порушення їхнього функціонування. Навмисні деструктивні електромагнітні впливи спрямовуються на руйнування інформаційних потоків, що циркулюють між елементами мережі; зниження швидкості інформаційного обміну між елементами системи керування, що істотно збільшує тривалість циклу керування і, як наслідок, знижує ефективність керування мережею; забезпечення достатньо масованого і довготривалого виведення з ладу мережних технічних засобів.

Ключові слова: інфокомунікаційна мережа; навмисні деструктивні електромагнітні впливи; електромагнітний тероризм; радіоелектронні інформаційно-технічні впливи; деструктивні ефекти.

Вступ

Постановка проблеми. Неядерні засоби генерації потужного електромагнітного імпульсу, здатного виводити з ладу електроніку, почали розробляти ще у часи Холодної війни. Відкрите обговорення проблеми навмисних деструктивних електромагнітних впливів (НДЕМВ) розпочалося з пленарної лекції професора В. Лоборєва на конференції AMEREM в 1996 році [1]. На симпозіумі з електромагнітної сумісності (ЕМС) у Цюріху 1997 року Комісія E URSI при своєму Комітеті з електромагнітного (ЕМ) імпульсу та пов'язаними з ним явищами, очолюваному М. Уіком, утворила підкомітет з ЕМ тероризму під керівництвом Х. Уіпфа. Перший огляд цієї проблеми опубліковано у пленарній доповіді Р. Гарднера на симпозіумі з ЕМС у Вроцлаві 1998 року [2]. Перший семінар «Електромагнітний тероризм і негативні наслідки високоенергетичних електромагнітних оточень» (Electromagnetic terrorism and adverse effects of high power electromagnetic (HPE) environments) з публікацією повних доповідей відбувся на симпозіумі з ЕМС у Цюріху 1999 року [3]. Слід зазначити, що на симпозіумі було представлено й важливі неопубліковані доповіді. Зокрема, доповідь віцепрезидента РАН академіка В. Є. Фортова, яка містила багато фотографій та технічних характеристик готових електромагнітних пристроїв високої потужності. Доповідь закінчувалася переконливим висновком (підкресленим М. Уіком під час закриття семінару), що для розв'язання проблеми ЕМ тероризму потрібне міжнародне співробітництво.

Навмисні деструктивні електромагнітні впливи, сформовані на основі наявних технічних засобів, є ефективним видом сучасних радіоелектронних інформаційно-технічних впливів на інфокомунікаційні мережі (ІКМ). Радіоелектронна матеріальна основа ІКМ є потенційно вразливою до впливу засобів НДЕМВ і, відповідно, є безпосереднім об'єктом такого впливу.

Завдання забезпечення якісного функціонування інфокомунікаційних мереж за умов впливів НДЕМВ потребують від системи керування мережею вірних і своєчасних керівних вирішень для запобігання небажаним наслідкам. Це зумовлює необхідність створення більш досконалих методів керування сучасними інфокомунікаційними мережами.

Мета публікації — розгляд уразливостей сучасних інфокомунікаційних мереж від навмисних деструктивних електромагнітних впливів, під якими за визначенням, прийнятим у міжнародній літературі, розуміють навмисне створення в злочинних або терористичних цілях потужного електромагнітного впливу на електронні та електричні системи для порушення їхнього функціонування.

Основна частина

Інфокомунікаційна мережа буде малоефективною, якщо через деструктивний вплив на неї відбудеться руйнування інформаційних потоків, що циркулюють між елементами мережі; зниження швидкості інформаційного обміну між елементами системи керування мережею, що призведе до значного збільшення тривалості циклу керування «виявлення загрози — ухвалення рішення — реалізація захисту» і, як наслідок, зниження ефективності керування; забезпечення достатньо масованого та довготривалого виведення з ладу мережних технічних засобів.

Залежно від поставленої задачі для формування навмисних деструктивних електромагнітних впливів можуть використовуватись мікрохвильові генератори високої потужності, генератори надширокосмугових сигналів та потужних електромагнітних імпульсів. Вражаюча дія електромагнітних імпульсів на мережу може бути зумовлена як безпосереднім впливом імпульсних електромагнітних полів на електричні та радіотехнічні кола, так і наведеними в сполучних лініях та колах струмами і напругами.

Логіка функціонування систем зв'язку традиційно декомпозується на сім функціональних рівнів відповідно до моделі відкритих систем — OSI (*Open Systems Interconnection*). Така декомпозиція дає змогу описати процеси передавання в системі зв'язку з різним ступенем функціональної абстракції — від фізичного рівня, на якому розглядається передавання сигналів у фізичному середовищі, до мережного та транспортного, на яких досліджуються процеси функціонування систем зв'язку в цілому. Водночас слід зазначити той факт, що значущими для опису процесів передавання в інфокомунікаційних мережах зв'язку є чотири нижні рівні моделі OSI (фізичний, канальний, мережний, транспортний), оскільки саме вони відповідають апаратно-програмним засобам мережі. Верхні рівні моделі OSI (сеансовий, представницький, прикладний) реалізуються програмними засобами абонента.

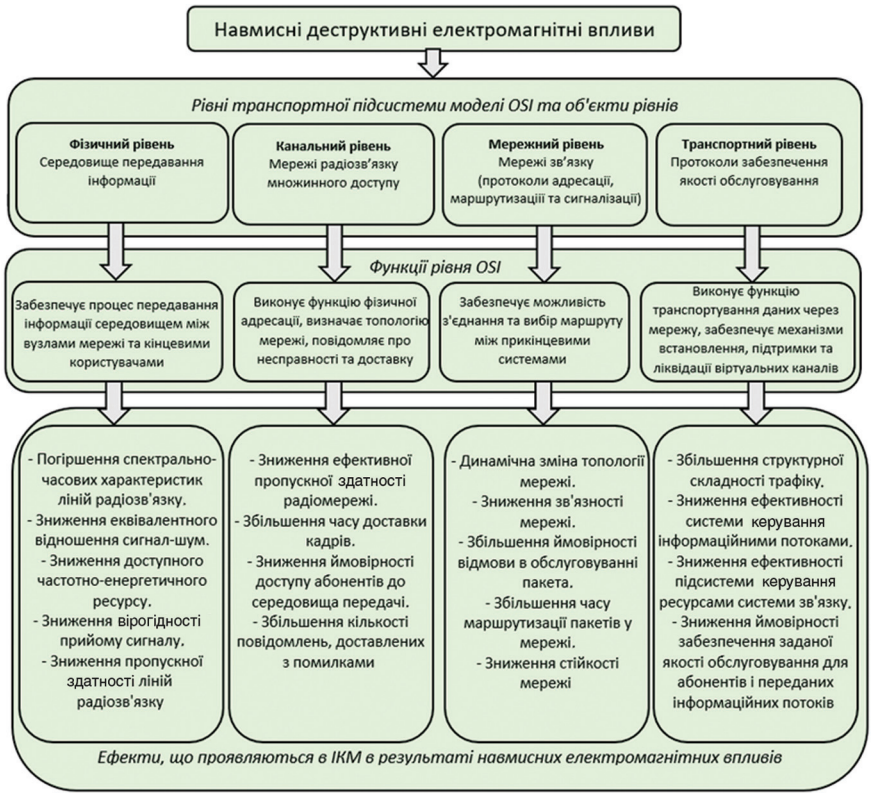
Сучасна методологія застосування «традиційних» засобів радіоелектронного пригнічення (РЕП) ставить за мету зниження якості обслуговування QoS (*Quality of Service*) окремих мереж та каналів радіозв'язку нижче значень, визначених вимогами до якості зв'язку. Отже, основну частину досліджень у галузі РЕП присвячено вирішенню завдань пригнічення об'єкта на фізичному рівні моделі OSI.

Об'єктами РЕП на фізичному рівні традиційно є радіоелектронні засоби та канали зв'язку. На канальному рівні OSI об'єктами пригнічення є канали множинного доступу, призначені для створення окремих радіомереж. До об'єктів деструктивного впливу на мережному рівні OSI належать вузли та канали зв'язку ІКМ, а також протоколи маршрутизації та сигналізації, що забезпечують процеси передавання даних. На транспортному рівні до об'єктів радіоелектронного впливу слід віднести протоколи та апаратно-програмні засоби забезпечення якості обслуговування інформаційних потоків, що передаються в ІКМ.

Аналізуючи можливості використання «традиційних» засобів РЕП [4], можна дійти висновку, що за їх допомогою можливі глибші впливи на ІКМ з метою порушення функціонування та інших об'єктів транспортної підсистеми моделі OSI (на фізичному, канальному, мережному і транспортному рівнях).

Перспективні способи РЕП, орієнтовані на пригнічення мереж, можуть використовувати ефекти деструктивного впливу на фізичному рівні як основу для формування ефектів пригнічення на канальному, мережному і транспортному рівнях моделі OSI. Вплив засобів РЕП на елементи ІКМ відбувається на фізичному рівні моделі OSI, але цей вплив повністю проявляється також на вищих рівнях транспортної підсистеми моделі OSI — канальному, мережному та транспортному. Саме завдяки використанню ефектів впливу засобів РЕП на канальному, мережному та транспортному рівнях OSI передбачається розв'язання проблеми комплексного пригнічення мережі.

Основні негативні ефекти на різних рівнях OSI, зумовлені впливом засобів РЕП, наведено на рисунку.



Ефекти, що проявляються на різних рівнях функціонування ІКМ у результаті навмисних деструктивних електромагнітних впливів

Нині в провідних країнах світу досягнуто істотних успіхів у розвитку засобів РЕП, що підвищило можливості останніх [5]. Здійснюється перехід від принципу пригнічення окремих елементів радіосегмента ІКМ (лінія радіозв'язку, мережа радіозв'язку) до використання цих елементів як своєрідних «точок входу» для радіоелектронних інформаційно-технічних впливів, які порушуватимуть мережні процеси передавання інформації та поширюватимуть свій дестабілізувальний вплив на всю ІКМ, зокрема і на її проводовий сегмент [6].

Дослідження ефектів впливу засобів РЕП на функціонування протоколів маршрутизації показали, що на мережному рівні ІКМ пригнічення окремих елементів мережі буде виявлятися як зниження ефективності функціонування алгоритмів маршрутизації, збільшення часу на встановлення з'єднань та доставляння пакетів, а також як зниження стійкості ІКМ [6].

Аналогічний ефект досягається під час формування складної структури інформаційних потоків, що циркулюють у мережі [4]. Це дає змогу зробити висновок про принципову можливість реалізації пригнічення ІКМ завдяки дестабілізації функціонування протоколів маршрутизації через вплив засобів РЕП на окремі мережі радіозв'язку.

З огляду на викладене в ІКМ має бути така організація системи керування, яка дає можливість реалізувати режим високої інформованості про ситуацію, що виникає в навколишньому середовищі завдяки формуванню та підтриманню цілісного й єдиного інформаційного простору, а також включення до процесу безперервної актуалізації інформації, котра отримується від якомога більшої кількості джерел первинної інформації.

У процесі формування рішення та керувальних впливів потрібне використання всієї доступної інформації в контурі ухвалення рішень, а також здатність формувати цілі всередині себе на основі високої поінформованості про ситуацію, що виникає в навколишньому середовищі.

Висновки

Потреба в забезпеченні якісного функціонування сучасних інфокомунікаційних мереж зумовлює необхідність розуміння вразливостей інфокомунікаційної мережі від дії на неї навмисних електромагнітних деструктивних впливів.

Наявні системи та способи РЕП зорієнтовано на пригнічення лише окремих каналів ІКМ через порушення функціонування протоколів зв'язку на фізичному та канальному рівнях моделі OSI.

У подальшому є загроза переходу до використання окремих елементів радіосегмента ІКМ як своєрідних «точок входу» для радіоелектронних інформаційно-технічних впливів, які порушуватимуть мережні процеси передавання інформації та поширюватимуть свій дестабілізувальний вплив на всю ІКМ, зокрема і на її проводовий сегмент.

Отже, слід зазначити, що в цій статті висвітлено лише деякі аспекти досліджуваної теми. Нині автори продовжують активні науково-дослідні роботи у цій предметній галузі. Проміжні результати досліджень щодо інформаційного забезпечення контролю поточного стану інфокомунікаційної мережі за умов впливу зовнішніх завад було опубліковано в праці [7], а питання оцінювання поточного стану інфокомунікаційної мережі на основі аналізу часових рядів — у статті [8].

Список використаної літератури

1. ***Loborev V. M.*** *The modern research problems // AMEREM Conference. Albuquerque, NM, 1996, May.*

2. ***Gardner R. L.*** *Electromagnetic terrorism. A real danger // Proc. of the 14th Int. Wroclaw Symposium on EMC, Wroclaw, Poland, June 23–25, 1998. P. 10–14.*

3. ***Workshop W4:*** *Electromagnetic terrorism and adverse effects of high power electromagnetic (HPE) environments // Supplement to Proc. of the 13th Int. Zurich Symp. on EMC. Zurich, Switzerland, February 16–18, 1999. P. 181–200.*

4. ***Makarenko S. I.*** *Informatsionnoe protivoborstvo i radioelektronnaia borba v setetsentricheskikh voinakh nachala XXI veka: monografiia [Information warfare and electronic warfare to network-centric wars of the early XXI century: monograph]. Saint Petersburg, Naukoemkie Tekhnologii Publ., 2017. 546 p.*

5. ***Осипов А. С.*** *Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП: учебник / под науч. ред. Е. Н. Гарина. Красноярск: Сиб. федер. ун-т, 2013. 344 с.*

6. ***Макаренко С. И.*** *Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями // Системы управления, связи и безопасности: электрон. версия журн. 2017. Вып. № 4. С. 15–59. URL: http://sccs.intelgr.com/archive/2017–04/02–Makarenko.pdf.*

7. ***Kriuchkova L. P., Tarasenko D. O.*** *Information Support of the Current State Control of Infocommunication Network in Conditions of External Interference Influence // World Science. 2021. 8(69).*

8. ***Крючкова Л. П., Тарасенко Д. О.*** *Оцінювання поточного стану інфокомунікаційної мережі на основі аналізу часових рядів // Зв'язок. 2022. №2. С. 7–11.*

L. P. Kriuchkova, D. O. Tarasenko

INFORMATION COMMUNICATION NETWORKS AS AN OBJECT OF INTENTIONAL DESTRUCTIVE ELECTROMAGNETIC INFLUENCES

Deliberate destructive electromagnetic influences formed on the basis of existing technical means are an effective type of modern radio-electronic information and technical influences on information and communication networks. The radio-electronic material basis of information communication networks is potentially vulnerable to the influence of means of radio-electronic suppression. The need to ensure the high-quality functioning of modern information and communication networks under the conditions of intentional electromagnetic destructive effects requires correct and timely management decisions from the network management system to prevent undesirable consequences, which necessitates the creation of more advanced management methods. The purpose of the publication is to consider the vulnerabilities of modern information and communication networks from intentional destructive electromagnetic influences, which is understood as the deliberate creation of a powerful electromagnetic influence on electronic and electrical systems for criminal or terrorist purposes in order to disrupt their functioning. The effects manifested at different levels of information communication network functioning as a result of intentional destructive electromagnetic influences are considered.

Based on the results of the research, the following conclusions can be drawn: intentional destructive electromagnetic influences are aimed at destroying information flows circulating between network elements; decrease in the speed of information exchange between elements of the control system, which significantly increases the duration of the control cycle and, as a result, reduces the efficiency of network management; ensuring sufficiently massive and long-term failure of network technical means; existing systems and methods of radio electronic suppression are focused on suppressing only individual channels of the network by disrupting the functioning of communication protocols at the physical and channel levels of the OSI model; in the future, there is a threat of transition to the use of individual elements of the radio segment of the information communication network as a kind of «entry points» for radio-electronic information and technical influences, which will disrupt the network processes of information transmission and spread their destabilizing influence on the entire network, including its wire segment. In the article presented to the readers, only some aspects of the researched topic are highlighted. Currently, the authors continue active research work in this subject area.

Keywords: infocommunication network; intentional destructive electromagnetic influences; electromagnetic terrorism; radio-electronic information and technical influences; destructive effects.