УДК 621. 618:519

Григорій Митрофанович Тіхонов,
Артем Сергійович Шолохов

СИЛОВЕ ІНФОРМАЦІЙНЕ ПОДАВЛЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ — ТЕХНІЧНА ОСНОВА ВЕДЕННЯ СУЧАСНИХ ВОЄННИХ ДІЙ

Дійсний момент часу характеризується активним дослідженням у розвинутих країнах світу системних концепцій ведення новітньої форми інформаційного протиборства — силових інформаційних конфліктів [1]. При цьому, ***силовий інформаційний конфлікт*** — складна сукупність протиріч техніко-ергатичних відкритих систем із слабопередбачуваною поведінкою, що складається у енерго-інформаційному просторі та забезпечує у воєнних діях інформаційну перевагу над противником шляхом застосування засобів силового деструктивного впливу на телекомунікації противника та захисту від аналогічного впливу своїх військ.

Невід'ємною частиною таких дій є складові силового інформаційного протиборства — радіо (РП), електромагнітне (ЕМП) та програмно-комп'ютерне подавлення (ПКП) (рис. 1) [1—4].

Однак, вирішення проблеми формування методології організації силового протиборства в умовах застосування нових видів деструктивного силового впливу ускладнюється відсутність систематизованих знань з узагальнення сутності, властивостей та підходів до практичного застосування великої кількості різнорідних типів засобів силового інформаційного подавлення (функціонального ураження) з урахуванням основних принципів побудови "закритих" телекомунікаційних систем (ТКС). Зауважимо, що під засобами силового інформаційного впливу будемо розуміти сукупність

Рис. 1. Нові складові силового інформаційного впливу у воєнних діях

спеціальних програмних ударних засобів, засобів радіоелектронної боротьби (РЕБ), електромагнітного (функціонального) ураження, технологій, інформації та дезінформації, що застосовуються для порушення інформаційної безпеки телекомунікаційних систем протиборчої сторони.

Мета статті — проаналізувати та систематизувати стан та тенденції розвитку засобів силового впливу на інформаційний обмін, визначити роль та місце таких нових видів подавлення телекомунікаційних систем, як радіо-, електромагнітне та програмно-комп'ютерне подавлення при веденні силових інформаційних конфліктів.

Радіоподавлення телекомунікаційних систем — це комплекс заходів у інформаційному конфлікті з порушення роботи телекомунікаційних систем та засобів управління зброєю противника шляхом: впливу активними та пасивними радіоперешкодами; застосування хибних радіолокаційних цілей і пасток, передачі в радіомережах повідомлень, що дезінформують; демонстраційної (оманної) роботи радіоелектронних засобів, зміни умов розповсюдження радіохвиль [3].

Сучасний стан телекомунікаційних систем військ (сил) та управління зброєю зазнав революційних змін у бік підвищення перешкодозахищеності ліній зв'язку, масованого застосування супутникових систем, комп'ютерних мереж, глобальної автоматизації усіх процесів управління військами (силами) та зброєю (рис. 2). Основними принципами побудови новітніх "замкнутих" телекомунікаційних систем є (рис. 2):

- інтегрованість по вертикалі і горизонталі, мережевий характер;
- формування у реальному масштабі часу єдиної картини оперативно-стратегічної (тактичної) обстановки;
- створення ситуативних мережевих комплексів управління розвідкою, РЕБ та комплексним вогневим ураженням;
- забезпечення повної ситуаційної обізнаності у тактичній ланці;
- створення окремої системи управління мережевими ресурсами;
- створення багаторівневих телекомунікаційних мереж передачі даних;
- висока перешкодозахищеність ліній зв'язку за рахунок втілення сигналів з поширенням спектра (адаптивна та багаторівнева програмна перебудова робочої частоти), широкосмугових сигналів (широкосмугові сигнали з фазовою маніпуляцією), використання сучасних методів кодування.

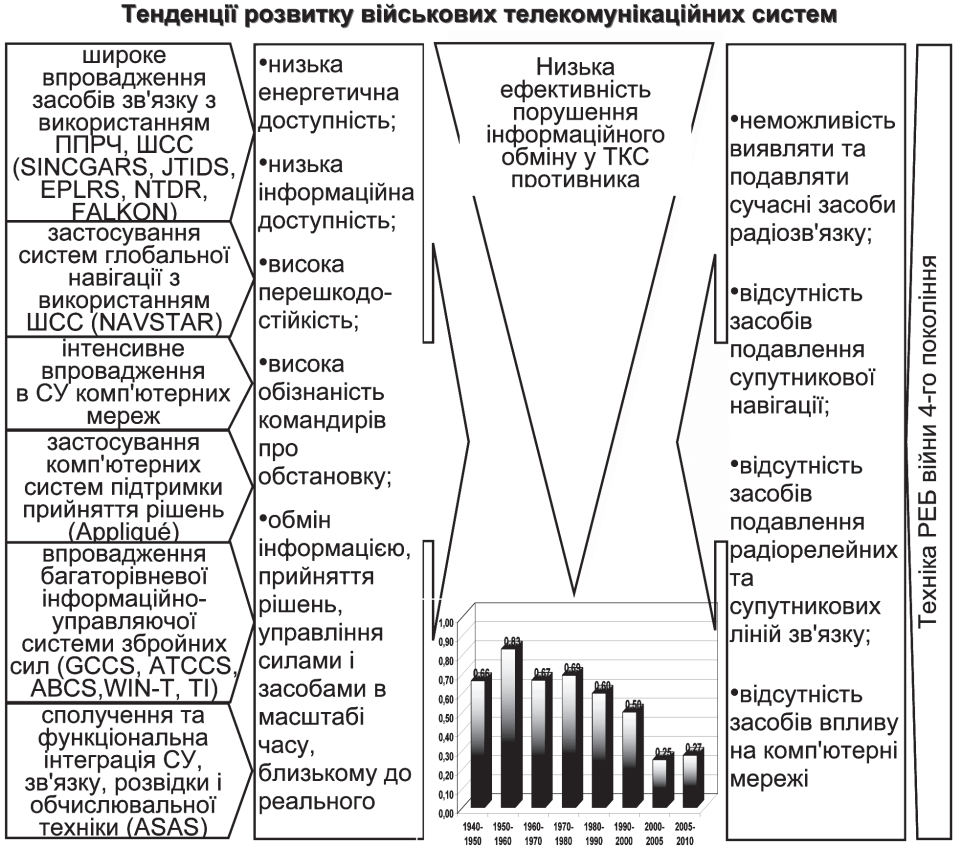

Рис. 2. Вплив тенденцій розвитку військових телекомунікаційних систем на ефективність порушення інформаційного обміну

Тому застосування традиційних засобів радіоподавлення у інформаційних конфліктах сучасності та майбутньому призводить до поступового зниження ефективності виконання завдань з порушення інформаційного обміну у військових телекомунікаційних системах (рис. 2).

Ефективне ведення сучасних інформаційних конфліктів у операціях неможливе без порушення функціонування:

- новітніх систем супутникового, радіорелейного та ультракороткохвильового зв'язку;
- радіокомандних систем наведення високоточної зброї (ВТЗ), телекомунікаційного забезпечення ситуативних розвідувально-ударних комплексів;
- розподілених сітчастих телекомунікаційних комплексів;
- систем стільникового та транкінгового зв'язку, ліній управління радіокерованої зброї.

Модернізація та проведення доробок техніки радіоподавлення старого парку у бік збільшення потужності випромінювання, оптимізації радіоперешкод, розробки та реалізації нових методів частотно-часового пошуку та обробки сигналів підвищить ефективність вирішення лише окремих часткових завдань та несуттєво вплине на загальну ефективність порушення інформаційного обміну противника.

Досвід ведення РЕБ збройними силами провідних країн світу, аналіз світових досягнень у цій галузі дозволяє зробити висновок, що технічною основою для вирішення завдань РЕБ у інформаційному протиборстві стає:

- малогабаритна техніка радіоелектронного подавлення, що має модульну структуру передавача перешкод, що заноситься типу "Бакай" (радіус подавлення до 500 метрів) (рис. 3);
- засоби радіоподавлення на безпілотних (безекіпажних) системах з елементами штучного інтелекту, що можуть забезпечувати автономний пошук об'єктів впливу;
- інтегровані ситуативні розвідувально-перешкодо-вогневі комплекси, що працюють у реальному масштабі часу в рамках реалізації на полі бою "електронно-вогневої" концепції ведення збройної боротьби.

Для вирішення завдань радіоподавлення елементів телекомунікаційних систем у інформаційних конфліктах можуть застосовуватись комплекси РЕБ типу:

- в короткохвильовому діапазоні — Р-378, Р-325 та їх модифікації (вид завадового сигналу — прицільний за частотою, загороджувальний за напрямком, дальність подавлення близько 50 км);
- в ультракороткохвильовому діапазоні — Р-934 Б, У (дальність подавлення до 400 км), Р-330 П, У, Б (дальність подавлення до 30 км, вид завадового сигналу — прицільний по частоті та загороджувальна за напрямком);
- для деструктивного інформаційного впливу на навігаційні системи ближньої навігації можливо застосовувати станції Р-388 і їх модифікації (дальність подавлення близько 400 км);
- як вплив на елементи перспективних систем супутникового зв'язку доцільно застосовувати засоби РЕБ типу Р-379-Д, -С, СпС-1.

Радіоподавлення багатофункціональних бортових радіолокаційних станцій (ББРЛС) можливо здійснювати із застосуванням комплексів СПН-30, СПН-40, СПО-8 (дальність дії від 15 до 150 км).

Для силового подавлення систем управління терористичних угруповань можуть застосовуватись малогабаритні передавачі перешкод типу "Бакай".

Рис. 3. Малогабаритна техніка РЕП

Електромагнітне подавлення телекомунікаційних систем [2, 3]. Основною альтернативою радіоподавлення телекомунікаційних систем у інформаційних конфліктах є новий вид деструктивного впливу на соціотехнічні елементи — електромагнітне подавлення. При цьому, ***електромагнітне подавлення*** — це комплекс заходів у інформаційному конфлікті з порушення роботи систем управління противника шляхом створення короткочасних електромагнітних випромінювань (ЕМВ) великої потужності для виведення з ладу радіоелектронних та енергетичних елементів телекомунікаційних систем.

Високотехнологічні засоби електромагнітної поразки (ядерної і неядерної природи) елементів телекомунікаційних систем — електромагнітні боєприпаси (ЕМБ) неядерної природи з радіусом дії від 0,2 до 10 кілометрів до 500 км і до 700 км при використанні ядерних боєприпасів, наприклад рис. 4—7.

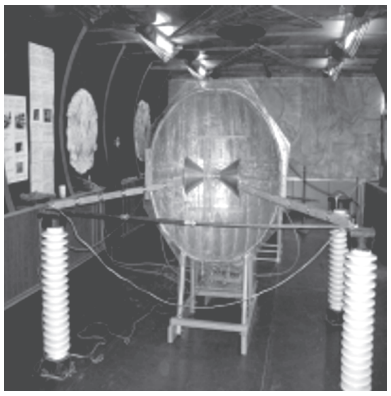

Рис. 4. Засіб ЕМП (дальність дії до 1500 м) (Україна)

Рис. 5. Засіб ЕМП (радіус дії до 500 м)

Рис. 6. Засіб ЕМП (радіус дії до 400 м)

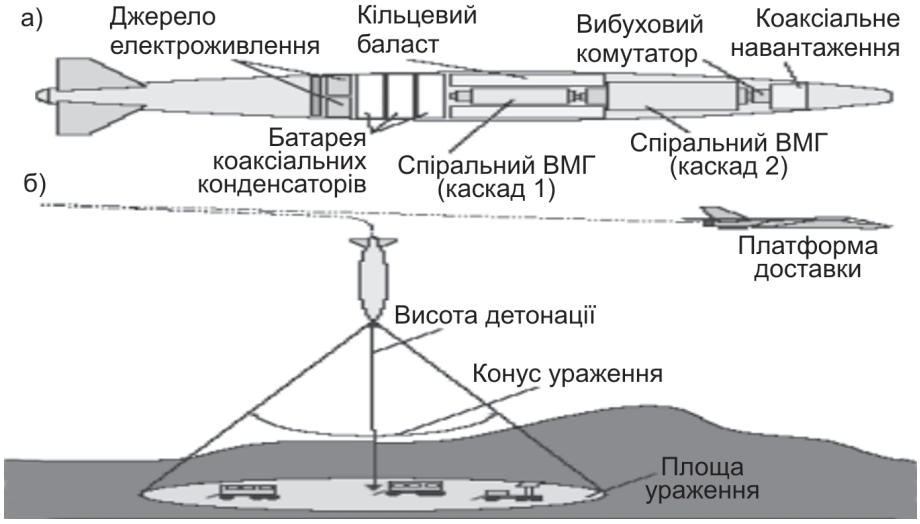

Рис. 7. Конструкція (а) і принцип бойового застосування (б) типового ЕМБ — Мк. 84 (900 кг)

Ключовими технологіями створення ЕМЗ є:

- генератори зі стиском потоку за допомогою вибухівки, що працюють на вибухівці або пороховому заряді;
- магнітогідродинамічні (МГД) генератори;
- мікрохвильові пристрої високої потужності, з яких найбільш сучасним є осцилятор з віртуальним катодом;
- SOS-генератори ЕМВ (Принцип дії SOS-генераторів базується на ефекті наносекундної комутації щільних токів у напівпровідникових пристроях (SOS — Semiconductor Opening Switch).

Вражаюча дія електромагнітних засобів. Низькочастотні електромагнітні засоби впливають на кабельну інфраструктуру (телефонні лінії, мережні і силові кабелі тощо). Діапазон напруг пробою для кремнієвих високочастотних приладів становить 15—65 В. Арсенід-галієві польові транзистори мають напругу пробою біля 10 В. Піддається впливу електромагнітного імпульсу комп'ютерна техніка та мережі.

Мікрохвильова зброя високої потужності, що працює у сантиметровому і міліметровому діапазонах, впливає на обладнання через вентиляційні отвори, щілини між панелями і погано екранованими інтерфейсами.

Дослідження показали, що опромінення площі діаметром у 400—500 м електромагнітними мікрохвильовими боєприпасами з висотою підриву в 4 км (генератор високої потужності 10 ГВт, 5 ГГц), призведе до ураження радіоелектронної апаратури у зазначеному радіусі. Радіус ураження комп'ютерної техніки — 1000...1500 м.

ЕМЗ для впливу на особовий склад у силовому інформаційному протиборстві. Американська компанія HSV Technologies разом з Каліфорнійським університетом розробила новий тип електромагнітних засобів — тетанайзери, або тетанизатори, що дозволяють тимчасово обезрушувати людину на відстані до 100 м (рис. 8).

Окремим напрямком є застосування ЕМЗ для створення больових відчуттів у особового складу. У ЗС США прийнятий на озброєння засіб, що нагріває шкіру людей мікро-

хвильовими променями, що одержав назву VMADS (Vehicle Mounted Active Denial System).

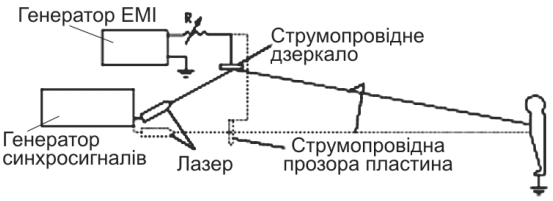

Рис. 8. Однопроменевий тетанайзер

Основними формами застосування високотехнологічних електромагнітних засобів у воєнних діях слід визначити: поодинокі електромагнітні впливи; групові електромагнітно-вогневі удари; масовані електромагнітно-вогневі удари; комбіновані форми застосування.

Програмно-комп'ютерне подавлення телекомунікаційних систем. Підвищення перешкодозахищеності засобів передачі даних, широке впровадження комп'ютерних радіомереж обумовило впровадження у інформаційне протиборство технологій, які базуються на руйнуванні обміну даних у комп'ютерних мережах. Наукові дослідження в цьому напрямі привели до появи в світовій практиці нового виду боротьби з телекомунікаційними системами — ***програмно-комп'ютерного подавлення (ПКП)*** [3, 4].

Проаналізуємо технічний, правовий і соціальний аспекти розвитку цього виду інформаційного протиборства.

Технічний аспект. Активний розвиток деструктивних програмних засобів і формування на їх основі арсеналу комп'ютерних атак на телекомунікаційні системи як спеціального, так і цивільного призначення. Наприклад, "вдала" комп'ютерна атака 21.11.2001, проведена на комп'ютерну мережу "Укртелекому" в Україні принесла збиток більше 1 мільйона гривень. У 2008 році успішно атакований сайт Президента України тощо.

Правовий аспект. Створення державами-монополістами в області інформаційних технологій правових основ для розвитку способів боротьби в інформаційному просторі. Відомо, що основою створення і функціонування комп'ютерних мереж (зокрема в Україні) є програмне забезпечення, що купується за кордоном. Однак уряди економічно розвинених країн обережно відносяться до експорту програмних продуктів і алгоритмів. Зокрема, законодавство США містить пункт 2778 "Контроль за експортом і імпортом озброєнь", на підставі якого діє інструкція "Правила контролю за переміщенням озброєння в світі" (International Traffic in Arms Regulations, ITAR). Розділ 120.1 ITAR відносить до військового спорядження програмне забезпечення. Прийнятий у 1992 рік білль S266 зобов'язав американських розробників криптографічних алгоритмів залишати "чорні ходи" для Агентства національної безпеки. Як наслідок — ослаблений криптографічний захист програмних продуктів, що експортуються.

Соціальний аспект. Використання соціальних суперечностей для монополізації ринку розробки і виробництва інформаційних технологій. Найбільш показовою для країн колишнього СРСР є проблема ***"электронного рабства"***. Великий відсоток науково-технічного потенціалу України, Росії, Білорусії через мережу Інтернет працює за символічну оплату на іноземні держави. Розвинені країни займають пріоритетне положення в плані акумуляції "мізків" в інформаційній сфері та накладають "інформаційне ембарго" на розвиток цих пріоритетних областей у небагатих країнах світу.

Програмно-комп'ютерне продавлення (ПКП) у інформаційному конфлікті — сукупність узгоджених за метою, завданнями, місцем і часом заходів і дій частин (підрозділів) інформаційної боротьби (розвідувально-диверсійних груп) з виявлення комп'ютерних засобів і радіомереж супротивника, здійснення доступу та впровадження до них спеціальних програмних засобів, які порушують нормальне функціонування комп'ютерних засобів і мереж, таємність та цілісність інформації, яка в них циркулює (рис. 9).

Можливими способами організації фізичного доступу до комп'ютерної мережі супротивника в операціях є: підключення до радіолінії передачі даних між комп'ютерами; підключення до кабельної лінії; фізичне захоплення терміналів.

Подолання процедури ідентифікації/аутентифікації в мережі полягає в підборі необхідної пари логін — пароль, який можливо здійснити методами пошуку і використання "ходів" у програмному забезпеченні сервера ідентифікації/аутентифікації (наприклад, ***"атака на переповнювання буфера"***), помилок конфігурації сервера ідентифікації/аутентифікації (програми типу Network Mapper), а також використання мережевого ***"сніфера"***, який виконує прослуховування, відбір пакетів даних і виділення хешированих паролів з наступним обчисленням дійсних текстових паролів (програми типу LC5, NetXRay).

Визначення топології мережі полягає в зборі інформації про підключені до мережі комп'ютери, їх функції, місцеположення і приналежність, а також уразливість. Для вирішення цих завдань проводиться сканування

мережі в цілому за допомогою програм типу Ping Sweep, Network Mapper, LanGuard, NetCrunch, Pinger і сканування портів певних комп'ютерів за допомогою програм типу Essential NetTools, Super Scan, Network Mapper. На основі отриманих даних і поставлених завдань визначаються основні і проміжні цілі (хости) і шляхи впливу на них.

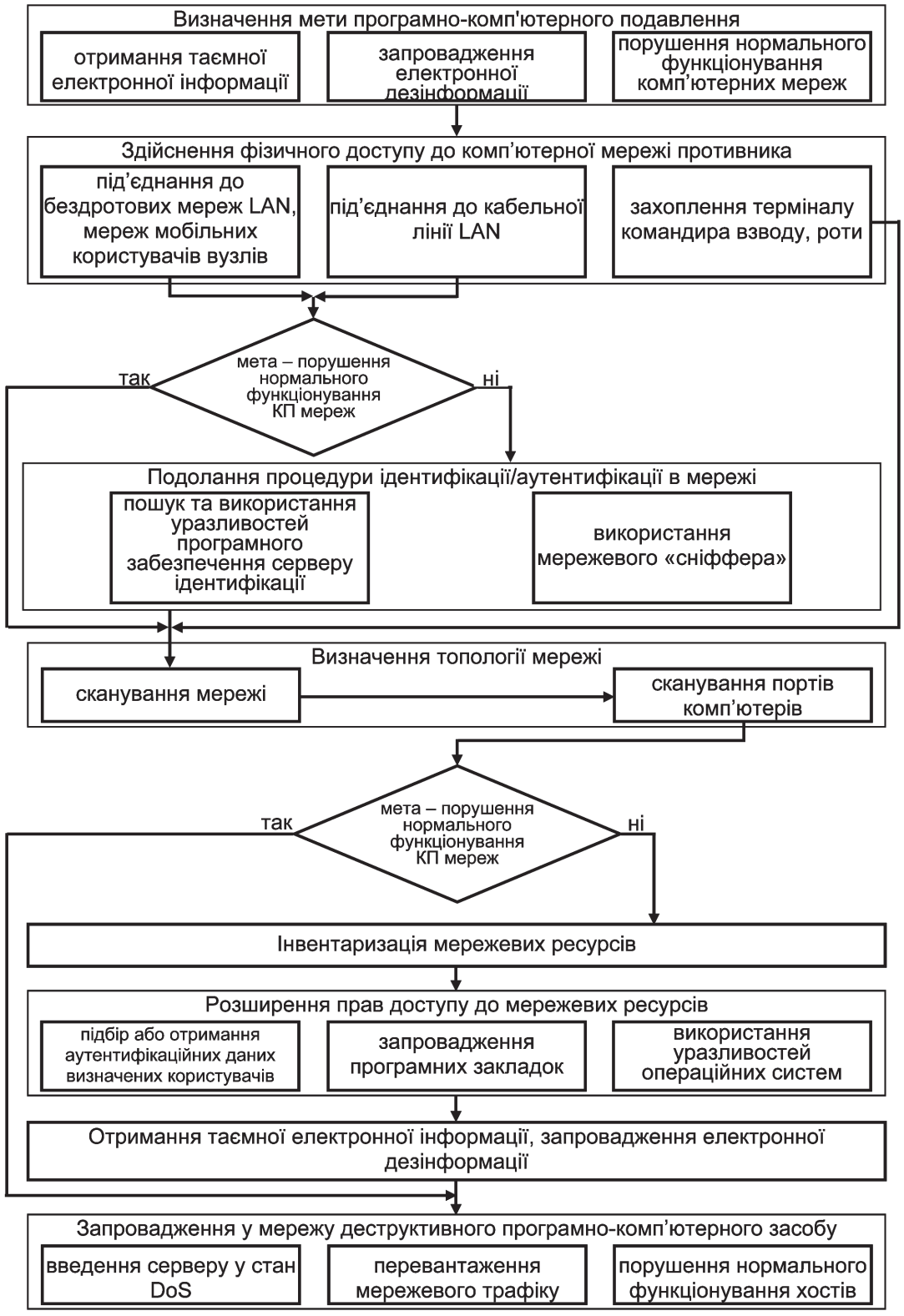

Рис. 9. Етапи програмно-комп'ютерного подавлення комп'ютерних мереж

Інвентаризація мережевих ресурсів полягає у визначенні списку облікових записів користувачів, їх прав доступу до певних ресурсів, а також самих ресурсів (устаткування загального користування, обчислювальні можливості, електронні бази даних, документи бойового планування, карти оперативно-тактичної обстановки і тому подібне). Виконання цього завдання бути здійснене за допомогою програм типу SMBGrind, LC5, Grinder, Legion, Essential NetTools.

Для розширення прав доступу до мережевих ресурсів можуть застосовуватися методи підбору або отримання аутентифікаційних даних певних користувачів (програми типу Getadmin), впровадження програмних закладок ("снифферов", троянських програм, реєстраторів натиснення клавіш), використання вразливості операційних систем (атаки типу SmbDie, Lovesan) [4].

Деструктивні програмно-комп'ютерні засоби впливу на програмно-математичне забезпечення. Це спеціальне програмне забезпечення комп'ютерні віруси, закладки, логічні бомби, троянські програми, черви та інші [3, 4]. Вірус по своїй структурі складається із двох частин — розмноження (цілеросподіл і доставку) і дій (бойової, ударної части). При цьому перша частина вірусу є ***"головкою наведення"*** і служить для вибору цілі (цілей) і доставляє його до об'єкта ураження. Інформація про цілі подається ***"системами комп'ютерної розвідки"***. При цьому системи і засоби впливу на програмне забезпечення можуть розглядатися як аналог ***високоточної зброї в інформаційному просторі.*** Ця частина вірусу може бути "міною повільної дії" і спрацьовувати при виконанні необхідних умов. Дуже часто "бойова" частина вірусу подана касетним зарядом, здатним вражати декілька об'єктів за один запуск.

Серед вірусів становлять інтерес ***віруси-розвідники*** для збору паролів системи, наприклад Trojan_psw_spion.

Метою комп'ютерної атаки може бути як порушення, так і захоплення управління засобами противника. Засоби для здійснення такої атаки — ***"троянські програми"*** (типу Backdoor.BO, aka Back Orifice Trojan) і NetBus [5]. Ці програми-утиліти віддаленого адміністрування комп'ютерів складаються з двох частин: видаленого "клієнта-розвідника" і "серверної" частини. Видалений "клієнт" діє по командах з центру і служить засобом (плацдармом) для ведення інформаційних дій. Ефективним засобом створення і розповсюдження деструктивних засобів є автоматизовані ***"конструктори вірусів"*** (наприклад, VLC, NRLG, PS-MPC, G2).

Засоби силового інформаційного впливу на телекомунікаційні засоби обміну даними. Це засоби перехоплення, руйнування або спотворення інформаційних масивів (масивів програм і даних), використовуваних у автоматизованих інформаційно-ударних системах супротивника). Згідно огляду NIST (http://www.nist.gov), найбільш популярними атаками на мережі і телекомунікаційні засоби обміну даними вважаються:

- установка вірусу на комп'ютер жертви за допомогою передачі файлу по ICO;
- застосування програм видаленого адміністрування;
- переповнювання робочого телекомунікаційного каналу користувача (атаки "відмова в обслуговуванні") шляхом відсилання йому величезної кількості TCP-пакетів з позначкою "терміново" (наприклад, за допомогою WINNUKE).

На рівні мережевого програмного забезпечення можливі: прослуховування каналу; перехоплення пакетів на маршрутизаторі; створення помилкового маршрутизатора; нав'язування помилкової інформації (пакетів).

Активно схильні до програмно-комп'ютерного придушення системи управління енергетикою, банками і подібні до них. Вже давно зрозуміло, що неможливо говорити про комп'ютерну безпеку незакритих комп'ютерних систем в Україні до тих пір, поки не буде розроблена "своя" операційна система. Застосування операційних систем, що купуються за кордоном, неминуче ставить важливі системи життєзабезпечення держави в стан очікування команди на виключення ззовні.

Із застосуванням описаних класів деструктивних програмних засобів можуть бути реалізовані різні види атак у рамках загального задуму ведення ПКП. Наприклад, ***введення сервера в стан DOS*** може бути досягнуте застосуванням атак типу Lovesan, SmbDie, ICMP Flood, SYN Flood, Pipe Bomb. Для ***перевантаження мережевого трафіку*** застосовуються "мережеві черв'яки", атака типу UDP Flood. ***Порушення функціонування хостів*** досягається застосуванням атак типу Land, SYN Flood, Lovesan, SmbDie, ICMP Flood, Pipe Bomb, Helkern.

Програмні засоби семантичного впливу впливають на якість і достовірність інтерпретації оператором (групою операторів) семантичної інформації. До семантичної зброї відносяться:

- системи і засоби семантичного пошуку (виявлення), модифікації (фальсифікації) і знищення;
- системи і засоби семантичного і криптографічного аналізу;
- системи і засоби семантичної і криптографічної дії.

Наприклад, до засобів семантичної зброї можна віднести ***Масго-віруси,*** що заражають документи (інформацію, дані) з автоматичним виконанням макросів. Спочатку цей клас вірусів заражає систему, в якій проводиться підготовка таких документів (наприклад, в Microsoft Word спочатку заражає основний шаблон системи — normal.dot), а потім виконує деструктивні дії над даними (знищуючи або модифікуючи).

Висновки. У інформаційних конфліктах сучасних воєнних дій засоби силового інформаційного впливу на ТКС є узагальненим симбіозом властивостей зброї масового ураження, ситуативних розвідувально-ударних комплексів і традиційних вогневих засобів ураження, максимальна ефективність практичної реалізації яких може бути досягнута тільки на основі оптимального за показником "ступінь дезорганізації управління — вартість — складність виконання бойових завдань" комплексування засобів РП, ЕМП, ПКП. При цьому, за масштабами впливу комплексне угруповання високотехнологічних засобів подавлення ТКС аналогічне засобам масового знищення, зберігаючи при цьому можливість завдання "хірургічних" високоточних ударів по елементах систем життєзабезпечення держави, збройних сил, свідомості людей. Застосування угруповань високотехнологічних засобів подавлення (функціонального ураження) ТКС найкраще відповідає прогнозованому безконтактному характеру збройної боротьби майбутнього.

Питання організації застосування угруповань засобів РП, ЕМП, ПКП не розглянуті у повному обсязі та є, на наш погляд, пріоритетним напрямом забезпечення національної безпеки України в інформаційній сфері. Це вимагає:

- створення на державному рівні умов для проведення в Україні скоординованих досліджень у області виробництва засобів РП, ЕМП та ПКП як наступального, так і оборонного призначення. Проведення маркетингових досліджень з конкурентоспроможності вітчизняних засобів РП, ЕМП та ПКП на світових ринках озброєнь;
- розробки науково-методичних основ моделювання інформаційного протиборства. Створення "дослідницьких полігонів" для практичного випробування наступальних засобів впливу на інформацію, як вітчизняних так і тих, що купуються за кордоном, програмних продуктів на стійкість функціонування в умовах РП, ЕМП та ПКП [5];
- упровадження вітчизняної операційної системи для забезпечення потреб ЗС України, СБУ, органів державного управління, енергетики, фінансів;
- розробки теоретичних основ комплексного ведення радіоелектронного, електромагнітного та програмно-комп'ютерного подавлення у сучасних воєнних діях, а також захисту своїх інформаційних систем від аналогічних видів впливу противника [5];
- створення в Україні багаторівневої системи підготовки та перепідготовки фахівців з питань розробки та організації комплексного застосування та управління угрупованнями засобів деструктивного силового впливу у інформаційних конфліктах воєнних дій.

Литература

1. Черниш О. М. Основи формування нової ідеології ведення радіоелектронної боротьби у війнах і збройних конфліктах майбутнього / О. М. Черниш, С. О. Тищук, С. М. Шолохов // Наука и оборона. — К., 2006. — № 4. — С. 48—51. **2. Шолохов С. М.** Електромагнітна зброя основа формування нової ідеології ведення РЕБ у сучасній збройній боротьбі та у майбутньому / С. М. Шолохов, С. О. Тищук // Волонтер. — 2005. — № 5 (37). — С. 18—21. **3. Шолохов С. Н.** Информационное оружие — новый класс вооружения для дезорганизации автоматизированных систем управления войсками и оружием при проведении информационных наступательных операций / С. М. Шолохов, С. А. Сидченко // Сб. научн. трудов ХВУ. — Х., 2002. — № 1 (39). — С. 10—17. **4. Шолохов С. Н.** Программно-компьютерное подавление / С. Н. Шолохов, Э. В. Лучук // Волонтер. — 2006. — № 2. — С. 18—22. **5. Певцов Г. В.** Наукові основи обґрунтування способів бойового застосування сил та засобів радіоелектронного подавлення в операціях / Г. В. Певцов, С. М. Шолохов, Г. М. Тіхонов, І. М. Тіхонов // Зб. наук. праць НДІУ і Н. — К., 2008. — № 4. — С. 48—51.

Статья посвящена тенденциям развития средств силового информационного подавление телекоммуникационных систем, определены роль и место новых видов подавления — радио-, электромагнитного и программно-компьютерного при ведении силовых информационных конфликтов современных военных действий. Сделан вывод, что в информационных конфликтах современных военных действий средства силового информационного влияния являются обобщенным симбиозом свойств оружия массового поражения, ситуативных высокоточных разведывательно-ударных комплексов и традиционных огневых средств поражения.

Ключевые слова: радиоэлектронная борьба, радиоподавление, электромагнитное подавление, программно-компьютерное подавление, информационный конфликт.

The article is devoted progress of facilities of power informative suppression of the telecommunication systems trends, a role and place of new types of suppression is certain — radio, electromagnetic and programmatic — computer at the conduct of power informative conflicts of modern military operations. A conclusion is done, that in the informative conflicts of modern military operations facilities of power informative influence are the generalized symbiosis of properties of weapon of mass defeat, situation high-fidelity reconnaissance-shock complexes and traditional fire weapons of defeat.

Key words: radio electronic fight, radio suppression, electromagnetic suppression, programmatic and computer suppression, information conflict.