1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації

Володимир Хорошко, Тетяна Козел, Ольга Ярошенко
Національний авіаційний університет
УДК 355.433.4:004.324 (045.5)

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ ЗБРОЇ

Анотація: **Розглядаються сучасні види інформаційної зброї, способи, методи та прийоми її застосування.**
Summary: **In the article the modern types of information weapons, methods, techniques of application.**
Ключові слова: **Інформаційна зброя, інформаційна війна, інформаційна боротьба, інформаційно-психологічний вплив.**

I Вступ

Значні досягнення за останні десять років в області комп'ютерних, інформаційних і телекомунікаційних технологій зробили світ уразливим перед новою зброєю, можливо, більш небезпечною, ніж ядерна. Мова йде про війну нового покоління – інформаційну, спрямовану не стільки на безпосереднє знищення супротивника, скільки на досягнення політичних цілей без ведення бойових дій, значимість якої останнім часом на теренах України стала доволі високою.

Під інформаційною війною, як стверджується в [1], у нових суспільних умовах слід розуміти інформаційне протиборство, "…що охоплює весь інформаційний простір супротивних держав…" й лиш відіграє роль певного узагальнюючого поняття усіх форм боротьби – починаючи з дипломатичної, економічної і закінчуючи збройною [1]. В індустріально розвинених країнах світу в широкому обігу воно з'явилось у другій половині 80-х років. Більш активно це поняття почало згадуватись уперше після проведення операції "Буря в пустелі" у 1991 році, де нові IT- технології вперше були використані як засіб ведення бойових дій. Нині під інформаційним протиборством розуміють закономірний об'єктивний процес у стосунках між протиборчими сторонами, спрямований на досягнення останніми цілей власної державної політики в мирний та воєнний час шляхом комплексного впливу на систему державного і військового управління протиборчої сторони та її військово-політичне керівництво, а також захист своїх інформаційних об'єктів від подібного впливу. Воно може проводитись у політичній, економічній, оборонній, науково-технічній та інших сферах шляхом: впливу на елементи інформаційно-телекомунікаційних систем з метою знищення елементів інфраструктури державного і військового управління; перехоплення і обробки відкритої інформації, що циркулює в інформаційних системах та друкується в засобах масової інформації (ЗМІ); несанкціонованого доступу до інформаційних ресурсів з їх наступним перекручуванням, знищенням або розкраданням; перехоплення і дешифрування інформаційних потоків, переданих каналами зв'язку, побічним випромінюванням або отриманих за рахунок впровадження спеціальних технічних засобів перехоплення інформації; формування та поширення інформаційними каналами протиборчої сторони або глобальних мережах дезінформації з метою впливу на оцінки, наміри та орієнтацію населення і особи, що приймає рішення тощо.

Так в сучасній війні неможливо досягти поставлених цілей без постійного здійснення заходів інформаційної боротьби не тільки в ході, але ж ще задовго до її початку та після завершення. Тому фахівці виділяють як самостійний вид зброї – інформаційну зброю, яка розглядається як засіб ведення інформаційної боротьби.

На сьогоднішній день інформаційна зброя є єдиною ефективною зброєю, яка в умовах науково-технічного прогресу здатна призвести одну з протидіючих сторін до перемоги, в той час, як застосування арсеналу сучасної традиційної зброї в глобальному або відносно глобальному конфлікті здатне призвести до знищення всіх учасників протистояння або, принаймні, до непоправних втрат в структурі національної безпеки, економіки та інших важливих сферах життєдіяльності конфліктуючих сторін такою мірою, що жодна з них не зможе скористатися результатами перемоги.

Застосування інформаційної зброї зводиться до таких способів як:

- вплив на окремі одиниці інформаційної системи супротивника з метою нанесення збитків;

- знищення або пошкодження цінних ресурсів противника, подолання систем захисту, впровадження вірусів, програмних закладок і логічних бомб;
- вплив на інформаційні ресурси інформаційних систем і систем управління з метою спотворення або модифікації даних;
- перехват каналів розповсюдження інформації супротивника з метою поширення дезінформації, чуток;
- вплив на персонал інформаційних і телекомунікаційних систем з використанням програмних засобів для введення інформації в підсвідомість або погіршення здоров'я людини;
- проведення терористичних дій.

Мета роботи – **в**изначення поняття та виду інформаційної зброї за об’єктом впливу, способи, методи, прийоми та особливості застосування інформаційної зброї в сучасних умовах.

II Основна частина

Зброя, як складова поняття – пристрої та засоби, вживані в збройній боротьбі для поразки та знищення противника. Поразка противника полягає в його знищенні (руйнуванні), придушенні та виснаженні (живої сили об’єктів).

Знищення противника передбачає завдання йому такого збитку, при якому він повністю втрачає боєздатність. Придушення означає завдання об’єкту такого збитку (пошкоджень) і створення для нього таких умов, при яких він тимчасово позбавляється боєздатності, обмежується (забороняється) його маневр або порушується управління. Виснаження полягає в тривалому веденні по противнику вогню обмеженою кількістю сил і засобів або завдаванні по ньому періодичних ударів авіації та артилерії. Основною його метою є морально-психологічний вплив на живу силу об’єкта й тим самим зниження його боєздатності та нормального функціонування.

На відміну від традиційної зброї, зброя інформаційна є суто наступальною, оскільки заходи щодо нейтралізації її впливу становитимуть заходи захисту, спрямовані на забезпечення власної інформаційної безпеки, а будь-які дії у відповідь, зміст яких складатиме використання інформаційної зброї (ІЗ), слід розцінювати як наступальні.

ІЗ має наступні ознаки:

скритність – можливість досягати мети без видимої підготовки і оголошення війни;

масштабність – можливість наносити непоправної шкоди, не визнаючи національних кордонів і суверенітету, без обмеження простору у всіх сферах життєдіяльності людини та суспільства;

універсальність – можливість багатоваріантного використання як військових, так і цивільних структур країни нападу проти військових і цивільних об'єктів цієї країни.

Критерієм віднесення до розряду інформаційної зброї може розглядатися ефективність того чи іншого озброєння при вирішенні завдань інформаційної боротьби. Доведено, що найбільших втрат збройні сили несуть від впливу вражаючих елементів інформаційної зброї, що діють на системи управління та психіку людини. Інформаційна зброя розглядається як засіб ведення інформаційної війни , що є лише ключовим елементом повномасштабної війни (гібридної війни).

Класифікація інформаційної зброї може бути проведена за наступними напрямками [2, 3]: за метою застосування; за об'єктами впливу; за механізмами реалізації впливу; за характером впливу на інформацію та інформаційні процеси; за масштабом вирішуваних завдань; за терміном дії тощо.

Завданням ІЗ є, за яскравим висловом М. А. Булгакова, «розруха в головах», яка небезпечніша за розруху в економіці, тому що втрата національних, духовних цінностей веде до виродження народу й краху суспільства.

Об’єктами ІЗ є: інформаційно-технічні та інформаційно-аналітичні системи, кожна з яких вміщує особистість; інформаційні ресурси; системи формування суспільної свідомості і думки, що базуються на засобах масової інформації і нарешті одним з основних об’єктів інформаційно-психологічного впливу є психіка і свідомість молоді, майбутнього нації.

Отже, за об’єктами впливу інформаційну зброю можна поділити на два основних класи [4]:

1. інформаційно-технічна зброя, що впливає на інформаційні ресурси, інформаційну інфраструктуру збройних сил, держави в цілому;

2. інформаційно-психологічна зброя, що впливає на морально-психологічний стан людини, соціальних та інших груп населення, суспільства в цілому.

Розглянемо та з’ясуємо найбільш поширені види інформаційної зброї за даними класами.

На сьогодні інформаційно-технічна зброя визначається як засоби знищення, викривлення або викрадання інформаційних масивів, видобування з них необхідної інформації після подолання системи захисту, обмеження або заборони доступу до них законних користувачів, дезорганізації роботи технічних засобів,

виводу з ладу телекомунікаційних мереж, комп'ютерних систем, усіх засобів високотехнологічного забезпечення життя суспільства і функціонування держави.

Програмно-технічна інформаційна зброя включає наступне:

Засоби несанкціонованого збору інформації**,** що дозволяють здійснити несанкціонований доступ до комп'ютерних систем, визначати коди доступу, ключі до шифрів чи іншу інформацію про зашифровані дані. Одна з найбільш поширених різновидів програмних продуктів несанкціонованого збору інформації є клавіатурні шпигуни. Такі програмні закладки націлені на перехоплення паролів користувачів операційної системи, а також на визначення їх легальних повноважень і прав доступу до комп'ютерних ресурсів. Крім того широко застосовуються різного роду програмні закладки як резидентних так і нерезидентних типів, віруси та інші засоби атак.

Як одну з можливостей протистояти сучасним загрозам в інформаційній сфері та сфері кібербезпеки британські програмісти запропонували оборонну кіберзброю – так званий "Internet-телескоп". Він відстежує проблемні зони мережі Internet і автоматично припиняє кібератаки. Проникаючи в "глибини" мережі, "телескоп" аналізує зміст трафіку (переданих даних) на предмет наявності злоякісних програмних кодів, які призводять до перетворення окремих зон мережі в ботнети, що складаються з уражених машин - "комп'ютерних зомбі".

Уражені машини, найчастіше без відома їхніх користувачів і власників, віддалено керуються зловмисниками та втягуються у виконання масових дій на кшталт розсилання спаму, навмисного створення надмірного числа запитів на ті чи інші сервери (Ddos атаки) з метою спровокувати їхню відмову тощо. Виявивши заражені вузли мережі, "телескоп" встановлює фізичне місце знаходження окремих "зомбованих" комп'ютерів і складає карту загроз, яка при бажанні може бути проаналізована фахівцями. У подальшому "телескоп" без зайвого втручання обслуговуючого персоналу визначає тип шкідливої програми й переводить її подальші дії під свій контроль. Це стало можливим завдяки реалізації в роботі "телескопа" алгоритму, який дає можливість виявити домени, що повинні стати об'єктом наступної атаки, "оточити" їх в такий спосіб, щоб нейтралізувати кібератаку. Після цього система або знищує бот-мережу, наказуючи підлеглим їй комп'ютерами прийняти виконання злоякісного коду, або розставляє пастку для її створювача. Порушивши програму, "телескоп" може спровокувати запит з комп'ютера – джерела атаки, "запеленгувати" його та подати сигнал місцевим правоохоронним органам. Як заявили представники британського уряду [2], відсутність таких та інших, "більш реалістичних" рішень, у сфері протидії ІЗ на критично важливу інфраструктуру може суттєво "…підштовхнути до міждержавної кібервійни в майбутньому…". Аналогічна позиція висловлена у доповіді Генерального секретаря Міжнародного союзу телекомунікацій на виставці ITU Telecom World у Женеві, у якій він визначив, що "…третя світова війна може початись як наслідок інформаційного протиборства…" [2]. При цьому за його ж словами майже будь-яка людина "…за допомогою армії заражених комп'ютерів ("ботнетів") зможе мати велику владу у такій віртуальній битві…".

Враховуючи таке й не зважаючи на те, що НАТО вже сьогодні має три лінії кібероборони, а саме: службу НАТО Computer Incident Pesponse Capabilities Centre; Гаазький дослідний центр перевірки діючих систем; вироблення нових стандартів захисту та Програму розробки захищених систем зв'язку, – керівництво Альянсу останнім часом з метою підвищення ефекту ведення воєнних дій у кіберпросторі додатково розробило:

- спеціальну структуру для захисту країн членів Альянсу від кібератак, яка займається збором розвідувальних даних і координує дії членів НАТО у боротьбі з кіберзлочинністю та ІЗ;
- концепцію кібервійни майбутнього [2, 3], в основу якої покладено перш за все військово-технічні концепції C^4I (Command, Control, Computer, Communications and Intelligence) та C^4IFTW (Command, Control, Computer, Communications and Intelligence for the Warrior), а також доктрину так званого кіберманевру, що передбачає поділ усього театру воєнних дій на дві складові – традиційні та кіберпростори.

Концепція C^4I передбачає погоджений розвиток систем управління, обчислювальної техніки, зв'язку та розвідки. Основним змістом цієї концепції є автоматизація різних процедур збору, обробки, зберігання і передачі інформації [2]. А концепція C^4IFTW [2] передбачає, перш за все, сполучення та функціональну інтеграцію систем управління, обчислювальної техніки, зв'язку та розвідки й, по-друге, створення глобальної інформаційно-управляючої інфраструктури, що повинно забезпечити умови для початку бойових дій викликаними військовими формуваннями без попереднього розгортання системи управління й зв'язку відразу після перекидання до місця призначення.

Наступна ІЗ включає [1, 2] засоби активного комп'ютерного впливу, що здатні порушити конфіденційність, цілісність і доступність інформації, а також функціонування інформаційних систем органів управління державних і військових об'єктів, промисловості, транспорту, зв'язку, енергетики, банків та інших установ шляхом безпосереднього втручання в роботу комп'ютерних систем.

Найбільш численною та небезпечною для ІТ-систем протиборчої сторони серед наступальних засобів є група активного впливу, тобто так звана атакуюча кіберзброя. До її складу входять: комп'ютерні віруси; програмні закладки та логічні бомби; електромагнітні пушки (портативні генератори електромагнітних випромінювань великої потужності); різноманітні пристрої постановки активних завад; засоби знищення, перекручування та розкрадання інформаційних масивів; спеціальні апаратні закладні пристрої.

За допомогою програм – крекерів здійснюється злом різних систем захисту шляхом модифікації захисного механізму в самому програмному забезпеченні. Крекери є вузько спрямованими програмами, в результаті яких можливий не тільки безперешкодний прохід в систему, а й вільне використання різних комерційних (захищених) версій програм. Після дії крекеру, як правило, відкривається доступ іншим загрозам, що порушує основні характеристики безпеки окремих компонент інформаційної системи.

За допомогою програмних закладок, які вбудовуються в мережеве або телекомунікаційне програмне забезпечення, що може стежити за всіма процесами обробки інформації в комп'ютерній системі, а також здійснювати установку і видалення інших програмних закладок.

Фізична зброя призначена виключно для впливу на елементи інформаційних систем.

Радіоелектронна зброя включає засоби радіоелектронного придушення, що в умовах сучасної війни саме їхнє застосування передує початку бойових операцій, - найважливіший елемент радіоелектронної боротьби, що покликані забороняти або утрудняти функціонування електронних засобів супротивника шляхом випромінювання, відбиття електромагнітних, акустичних і інфрачервоних сигналів. Засоби радіоелектронної розвідки включають пасивні пристрої пошуку, перехоплення та аналізу радіовипромінювань та пеленгування джерел електромагнітних випромінювань; активні радіолокаційні та лазерні засоби спостереження, виявлення та розпізнавання; оптико-електронні прилади та інші прилади реєстрації фізичних полів об'єктів. Основною задачею є контроль дій супротивника в межах його інформаційної системи [1].

Інформаційно-психологічна зброя (ІПЗ) – тобто, сукупність спеціальних засобів і технологій, що використовуються для насильницького викривлення інформаційно-психологічного простору супротивника спеціально для ураження індивідуальної і масової свідомості. Знаючи головні характеристики відповідної спільноти – від демографічних до соціально-економічних, визначивши пануючі психотипи, розуміючи менталітет, на базі певних технологій можна активно впливати на цільову групу, модифікувати суспільну свідомість і формувати громадську думку, і, відповідно до конкретних цілей, провокувати, спонукати, збурювати до певних дій або дезорієнтувати і дезінтегрувати як окремі соціальні групи, так і цілі народи [4, 5].

ІПЗ за формою впливу можна класифікувати умовно так:

- психотронні засоби, які, через застосування відповідного випромінювання, порушують психічний чи психофізіологічний стан, впливають на сприйняття реальності, створюють неможливість адекватно реагувати на ситуацію;
- психотропні засоби, які через застосування певних біологічних чи хімічних реагентів впливають на психосоматику, змінюють загальний психофізіологічний стан особистості, погіршують її самопочуття і розумові здібності, викликають депресію чи панічний страх, галюцинації тощо.

Навіювання і гіпноз, НЛП (нейролінгвістичне програмування), інші техніки сугестивного впливу. Тут використовуються особливості людської психіки, завдяки яким особистість може піддаватися навіюванню і програмуванню. Передбачається директивність, тобто категоричність і обов'язковість виконання наказу (у випадку прямого навіювання) і неусвідомлене беззастережне виконання (під час гіпнотичного впливу). НЛП застосовує методики розщеплення свідомості, дисоціацію, збентеження тощо для позасвідомого введення в індивідуальну і масову свідомість певної інформації. Побудова асоціативних зв'язків і програмування через "якоріння", використання метафор та інших методів "мови несвідомого".

В умовах, коли застосовується ІЗ, можна застосовувати наступний алгоритм, що здавалось би "завжди перемагає" [6]:

1) визначення базових елементів інформаційного простору супротивника;
2) визначення індивідуальних особливостей і потенційних можливостей базових елементів;
3) моделювання різних варіантів поведінки базових елементів при різних вхідних впливах;
4) вибір найбільш переважного сценарію ведіння базових елементів;
5) підготовка середовища, в якому функціонують базові елементи (громадські думки), і їх самих;
6) реалізація.

Причому, що цікаво, подібний алгоритм цілеспрямованого інформаційного впливу, можна сказати в зародковому праобразі сьогоднішньої інформаційної війни, складений майже більш як сто років в документі під назвою "Протоколи зборів сіонських мудреців". Не вдаючись у суперечки про причини і джерела даного документа, хотілось би позначити, що його автора безперечно слід назвати серйозним теоретиком в області побудови типових тактик і стратегій ведення інформаційних війн і ІЗ [7].

У названому документі можна прочитати наступне

"В руках сучасних держав є велика сила, яка створює рух думки в народі – це преса".

Коротко і точно в "Протоколах…" сказано практично про всі аспекти інформаційної війни:

- система управління (контроль владних структур);
- кошти перепрограмування населення (засоби масової інформації);
- тероризм;
- економічні війни, засоби економічного управління;
- фінансова програма;
- загальне голосування і т. д.

Дані "Протоколи.." носять методичний характер. Вони складені так, що їх може використовувати будь-хто, розуміючи значення таємної війни, і зовсім не обов'язково обмежувати їх застосування тільки мудрецями і тільки тим далеким часом. З точки зору значущості для теорії інформаційної війни дані "Протоколи.." і аналогічні перші боязкі дослідження з теорії ядерної зброї відносяться приблизно до одного часу.

З того часу змінилося багато методів і прийомів, вони отримали наукове обґрунтування. Виникли цілі наукові дисципліни та напрямки про те, як управляти поведінкою людини, колективу, суспільства. До них відносяться: соціологія, психоаналіз, теорія реклами, суггестологія, діанетика і т. п. Отримав своє теоретичне обґрунтування гіпноз, і були зроблені спроби перенесення методів гіпнотичного впливу з окремого індивідуума на колективи і на цілі людські суспільства. Виробництво та розповсюдження інформації сьогодні поставлено на конвеєр. Всього цього ще не було навіть у минулому столітті, не було достатньо ефективних засобів масової інформації, не було науково обґрунтованих алгоритмів управління соціумами, а виникнення цих алгоритмів могло бути лише з появою теорії програмування для сьогоднішніх засобів обчислювальної техніки. Бо здійснити інформаційну операцію – це значить, що необхідно так підібрати вхідні дані для системи, щоб активізувати в ній певні алгоритми, а в разі їх відсутності – активізувати алгоритми генерації потрібних алгоритмів.

Наявна на сьогоднішній день теорія алгоритмів цілком дозволяє пояснити, яким чином може здійснюватися автоматичне написання програм для певних предметних областей. Процес наведення гіпнотичного стану на окреме суспільство міг, напевно, виглядати таким чином:

1) розслабити суспільство – вселяти через засоби масової інформації, що ворогів не має, при цьому обговорювати окремі історичні періоди та інтереси окремих народностей (мета – суспільство як ціле повинно зникнути як об'єкт свідомості суспільства);

2) змусити суспільство слухати тільки супротивника, не звертаючи уваги на якісь інші думки або відчуття, наприклад, акцентувати засоби масової інформації виключно на якість одній парадигмі суспільного розвитку (наприклад, "руський мир"), виключивши будь-який інший досвід (мета – процес завантаження суспільної свідомості; дія формуючих сил послаблюється);

3) змусити суспільство не розмірковуючи над тим, що говорить супротивник, для цього виключити із засобів масової інформації серйозні аналітичні дослідження проблем (мета – сприяти гальмуванню безперервного потоку думок);

4) зосередити увагу суспільства тільки на якомусь предметі крім вхідного інформаційного потоку, наприклад, внутрішні катаклізми, війни, акти терору. Мета такого процесу створити умови, для яких підсистема захисту, відповідальна а обробку вхідної інформації, виявляється не в змозі виконувати свою функцію;

5) постійно навіювати, що саме суспільство стає краще і краще, що всі навколишні ставляться до нього краще і краще (мета – подібне навіювання послаблює історичну пам'ять і почуття самоототожнюваності, якими характеризується нормальний стан суспільства);

6) ЗМІ одночасно повинні переконувати членів суспільства, що викликало стан – це не зовсім те, що повинно бути (мета – створення пасивного стану свідомості, в якому зберігається можливість залежності від інформаційного впливу супротивника).

Наведений алгоритм в загальних рисах відображає роботу ЗМІ в Росії часів 1990-1997 років та зараз, а також на Донбасі і в Криму.

Лінгвістичні методи і засоби. Передбачається цілеспрямоване використання певних мовних особливостей, тих чи інших спеціальних зворотів, спеціальної термінології, семантично однозначно не визначеної інформації тощо.

Символьно-семантичний апарат впливу, в тому числі віртуальний символізм, передбачає використання справжніх і штучно сформованих символів, здатних активувати у суб'єкта (перш за все – підсвідомо) певні смисли.

Загальна система обмеженого доступу до інформації передбачає примусове відчуження певної категорії інформації з міркувань державної і суспільної необхідності. Обмеження доступу встановлюється грифами на кшталт "державна таємниця", "особливо важливо", "цілком таємно", "таємно" тощо. Застосовується криптографія, тобто шифрування і дешифрування інформації.

Технології заданого інформування – це сукупність маніпулятивних дій з інформацією для здобуття переваги над об'єктом впливу через дозоване цілеспрямоване інформування, ініціалізація навмисних витоків інформації, введення опонента в оману тощо. Дезінформація, як правило, подається в достовірному контексті, семантично різноплановому; має певну ешелонованість, тобто глибину наповнення, що підвищує її вірогідність.

Цензура являє собою систему нагляду за діяльністю видавництв і ЗМІ. Передбачає загальне управління інформаційним простором з боку суб'єкта, наділеного владним ресурсом.

Пропагандистська діяльність націлюється на формування певного світосприйняття, морально-етичних норм, створення міфів та зразків наслідування через аудіо- і відеопродукцію, підручники, словники, енциклопедії тощо.

Засоби масової комунікації (ЗМК) – головне знаряддя в пропагандистських війнах. Масові заходи, особливості створення натовпу та керування ним передбачають певні передумови, де визначальне місце сьогодні також належить мас-медіа. Саме вони стимулюють короткочасні шаблони поведінки і довготривалі конвенції, що впливають на суспільство.

Слід зазначити і те, що всі розробки в галузі спеціальних психотронних технологій, спрямовані на досягнення ефекту на біофізіологічному рівні, не можуть навіть сукупно зрівнятися за своєю дієвістю із традиційними й цілком легальними ЗМК – передусім, власне мас-медіа, а також неформальним спілкуванням у формі чуток, пліток, анекдотів та приказок, що створюються штучно й націлюються на "ураження" суспільної свідомості. Оскільки масова свідомість завжди перебуває в очікуванні підказки, вони закономірно перебирають на себе роль головного "підказувача" [6].

Слід виокремити психотронні і психотропні технології внаслідок винятковості їх впливу, водночас зауваживши, що розробки в галузі частотного кодування мозку, хімічних і біологічних засобів, здатних викликати у людини психічні, психофізіологічні чи психологічні порушення, нездатність до адекватних дій, все ж не можуть зрівнятися з можливостями засобів масової комунікації, тобто мас-медіа як різновиду формальної комунікації, агітаційно-пропагандистських засобів та засобів неформальної комунікації (в першу чергу – чуток, пліток, анекдотів, приказок). Так, ефективність засобів масової комунікації перевищує всі вищезгадані засоби, взяті разом. Масова свідомість завжди очікує підказки, і роль головного підкажчика виконують засоби масової комунікації.

ІІІ Висновки

Бурхливий розвиток науки і техніки, засобів і способів комунікації, вдосконалення технологій інформаційного і психологічного впливу на людину сприяють виникненню нових видів зброї, заснованих на нових концептуальних, технічних, фізичних і технологічних принципах її застосування.

Інформаційна зброя цілком може розглядатися як альтернатива до зброї традиційної, а не її модифікація. Оскільки здійснення інформаційного впливу на супротивника є одночасним з веденням перших традиційних війн, не можна вести мову про те, що з використанням інформаційної зброї традиційна війна стає інформаційною.

В сучасному розрізі застосування інформаційної зброї здійснюється відповідним чином залежно від об'єкту впливу – інформаційно-технічна зброя, інформаційно-психологічна.

Однією з найбільш характерних особливостей інформаційно-психологічної зброї є її латентний характер, коли об'єкт не підозрює, що проти нього застосовується ця зброя. А якщо він і розуміє це, то завдяки домінуванню протиборчої сторони в інформаційній і психологічній сферах об'єкт впливу нічого не може протиставити.

Список використаної літератури: ***1.*** *Левченко О. Завдання, об'єкти та форми ведення інформаційної боротьби/Левченко О.//Вісник воєнної розвідки. — К.: ВДА ГУР МОУ України, Вип.21, 2010. — С.7-11.* ***2.*** *Роговский Е. А. Пентагон усиливает кибероборону/Роговский Е.А., Шариков П.А.//Научный и общественно-политический журнал "США – Канада. Экономика – политика – культура", №1, январь 2011. — С.51-60.* ***3.*** *Шафранський Р. Теорія інформаційної зброї. / Пер. В. Казеннова. — М:ВИКА, 2002,189 с.* ***4.*** *Історія інформаційно-психологічного протиборства : підруч. /[Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов В. М. Петрик, М. М. Присяжнюк, Є. Д. Скулиш]/ — К. : Наук. —вид. відділ НА СБ України,*

2012. — 212 с. ***5****. Пригожин А. И. Особенности четвертой мировой войны // Вестник Московского университета. Сер. 18. Социология и политология. — 2004. — № 3. — С. 60.* ***6.*** *Почепцов Г. Г. Информация и дезинформация. — К.: Ника-Центр, Эльга, 2001. — 256с.* ***7.*** *Панарин И. Н. Технология информационной войны. — М.: „КСП+”, 2003. — 320 с.*

Михайло Прокофьєв, Вадим Куліш, Микола Ващенко, Володимир Дворський, Василь Стеченко, Андрій Тодоренко
НДЦ «ТЕЗІС» НТУУ «КПІ»
УДК 004.056

ОЦІНЮВАННЯ КОЕФІЦІЄНТА ЯКОСТІ ШУМОВОЇ ЗАВАДИ В СИСТЕМАХ АКТИВНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Анотація: **Розглянуто методи оцінювання значень коефіцієнта якості шумової завади в системах активного захисту інформації, запропоновані рекомендації щодо удосконалення процедури його оцінювання з використанням методу визначення ентропії сигналів завад, який легко на практиці реалізується з використанням осцилографа з вбудованим процесором.**
Summary: **The methods of evaluation values of the noise disturbance as active systems of information protection offered recommendations for improving the procedures for its assessment using entropy method for determining signal noise that is easily implemented in practice using an oscilloscope with a built-in processor.**
Ключові слова: **Побічні електромагнітні випромінювання, просторове зашумления, маскуючі завади, энтропія, коефіцієнт якості шуму.**

І Вступ

Захист інформації, що обробляється на об'єктах інформаційної діяльності (ОІД), заснований на ослабленні або маскуванні рівнів побічних електромагнітних випромінювань і наведень (ПЕМВН) на границі контрольованої зони (КЗ). Це забезпечує зменшення співвідношення рівнів інформативний сигнал/шум у місцях можливого розташування засобів технічної розвідки (ЗТР). Використання цього активного захисту полягає у формуванні та випромінюванні на ОІД сигналу завади, рівень якого за потужністю перевищує рівні ПЕМВН і завдяки цьому перешкоджає прийманню і виділенню інформаційного сигналу ЗТР. Для виключення перехоплення ПЕМВН по електромагнітному каналу використовується просторове зашумлення, а для виключення знімання наведень інформаційних сигналів з провідних ліній - лінійне зашумлення.

Для ефективного захисту необхідно, щоб діапазон частот створюваних маскуючих завад охоплював весь частотний діапазон можливих ПЕМВН, завади не повинні мати регулярних спектральних складових, а на границі КЗ рівень завад повинен забезпечувати співвідношення рівнів інформативний сигнал/шум не більше допустимого значення, що визначається нормативними документами системи ТЗІ. Рівень завад не повинен перевищувати допустимих норм щодо електромагнітної сумісності і санітарно-гігієнічних норм.

У системах просторового зашумлення в основному використовуються завади типу «білий шум» з енергетичним спектром, близьким до рівномірного, з спектральною щільністю потужності, достатньою для надійного маскування ПЕМВН. Завдяки своїй універсальності такі системи одержали більш широке поширення порівняно з пасивними методами захисту, оскільки жодним чином не прив’язані до конкретного ОІД .

Основні технічні характеристики джерел маскуючих завад – генераторів шуму (ГШ), що застосовуються у сфері ТЗІ, характеризуються значеннями: спектральної щільності амплітуд електричної E_i та ρH_i магнітної компонент електромагнітного поля (ЕМП) шуму в робочому діапазоні частот, коефіцієнта K міжспектральних зв’язків, що враховує кореляційний зв’язок огинаючої однієї з обраних ділянок спектра ЕМП шуму з огинаючими решти ділянок спектра всередині частотного діапазону; коефіцієнта якості шуму γ, що враховує відмінність щільності ймовірностей $p(x)$ розподілу миттєвих значень амплітуд компонент E_i і ρH_i ЕМП шуму від щільності ймовірностей їх нормального гаусового розподілу.

У статті розглянуті теоретичні і практичні методи оцінювання і обчислення коефіцієнта якості шуму ГШ просторового і лінійного зашумлення, що використовуються для захисту ОІД від витоку інформації каналами ПЕМВН. Метою роботи є аналіз математичних моделей оцінки коефіцієнта якості шуму і вибір моделі, придатної для практичного використання у сфері ТЗІ.