УДК 004. 056 **А.В. Дудатьєв**

ІНФОРМАЦІЙНА ОБФУСКАЦІЯ: МЕТОДИ І МОДЕЛІ

Інформаційні війни є ефективним елементом проведення протиборства між конкуруючими сторонами. Життєдіяльність сучасного об'єкта захиступов'язана з рішенням важливої задачі – забезпеченням комплексної інформаційної безпеки, важливим компонентом якої є захист від проведення спеціальних інформаційно - психологічних операцій. В статті розглянуто поняття інформаційної обфускації, як технології заплутування людини. Запропоновано моделі для реалізації інформаційної обфускації, а також для оцінювання ефективності проведення спеціальних інформаційно - психологічних операцій. Представлені моделі пропонується використовувати у структурах інформаційно-аналітичних центрів по управлінню інформаційною безпекою на рівні "підприємство-регіон-держава"

Ключові слова: інформаційна війна, інформаційно-психологічна операція**,** інформаційна обфускація, інформаційний мем.

Вступ і постановка задачі

Проведення інформаційно-психологічних операцій **(**ІПО) передбачає системне використання комплексу різних методів, моделей, механізмів і заходів з метоюформування потрібної моделі світу. Ця модель складається з певних стереотипів поведінки, відношення досуспільства, відношення до отриманої інформації. Процес зміни оцінок, поглядів людей які приймають рішення, може створити умови точкового зовнішнього управління різноманітними процесами. Реалізація цієї моделі дозволяє в свою чергу розв'язувати інформаційні війни які є елементами так званих гібридних війн і які можуть бути реалізовані на будь-якій території. Тому актуальною задачею є реалізація комплексного інформаційного захисту соціотехнічних систем (СТС) суть якого полягає у інтегрованому захисті від інформаційно-кібернетичних операцій (ІКО) і інформаційно-психологічних операцій (ІПО) або іншими словами захисту власних інформаційних ресурсів і захисту від деструктивного інформаційного впливу. Однак, для побудови ефективногокомплексного захисту, зокрема захисту від ІПО необхідно ідентифікувати методи і технології проведення таких операцій,метою яких є маніпуляція свідомістю соціальної складової СТС.

Метою даної роботи єрозробка математичних моделей для оцінювання ефективності проведення інформаційної обфускації, як технології заплутування людини шляхом реалізації спеціальних інформаційно-психологічних операцій.

Огляд відомих результатів

Аналіз низки робіт показав, що досліджені лише окремі механізми та наслідки проведення ІПО. У роботі [1] розглянуто рефлексивне управління, яке відбувається шляхом нав'язування хибної мотивації. Існує ще один важливий аспект рефлексивного управління.С. Леоненко стверджує, що у багатьох випадках рішення приймають машини, які не здатні як людина реагувати на оточуюче середовище. В цьому випадку відбувається вплив на технічні засоби збору, обробки, передавання і відображення інформації з метою нав'язування опонентам своїхпоглядів. Тобто тут фактично мова іде про вплив програмно-технічної складової на людину і як наслідок на процес підготовки і прийняття рішення. Відомі роботи, що базуються на понятті мем, яке вперше ввів англійський вчений біолог Річард Доукінс. У цих роботах запропонований підхід який дозволяє виконати оцінку рівня загроз інформаційних викликів в інформаційному просторі соціально-телекомунікаційних систем[2]. Мем визначається як мінімальна кількість інформації у свідомості людини. Іншими словами, мемом можна назвати спеціально створене інформаційне повідомлення, яке розповсаджується у інформаційному просторі і яке призначене для формування необхідної моделі поведінки і прийняття відповідних рішень людиною. Сформувався навіть цілий науковий напрямок – меметика, яка власне і займається дослідженням таких процесів.Але відсутні роботи у яких досліджено можливість використання того чи іншого типу ІПО або їх

можливих комбінацій та наслідки їхдеструктивного впливу на об'єкт проти якого вони спрямовані.

Основна частина

Як вище було зазначено метою проведення ІПО є створення нової «моделі життя»для соціальної складової СТС шляхом донесення неправдивої або відповідним чином представленої правдивої інформації або комбінації правдивої і неправдивої інформації. Механізм заплутування людини яка складає соціальну складову СТС фактично нагадує технологію програмної обфускації, тобто технологію заплутування хакера від зламу програмного забезпечення. Суть процесу обфускаціїї полягає у тому, щоб знищити логічні зв'язки у об'єкті аналізу, наприклад, у програмному коді і таким чином максимально ускладнити процес вивчення і сприйняття або модифікації відповідної інформації. Так само і реалізація інформаційної обфускації може використовувати чутки, представлення інформації яку важко перевірити і відповідно спростувати і таким чином практично знищити логічні зв'язки між спеціально підготовленими інформаційними повідомленнями – мемами. Сучасні інформаційні технології дозволяють дуже оперативно і ефективно впливати на свідомість людини, її переконання шляхом спрямованого редагування інформації, яка циркулює наприклад у соціальних мережах, дублювання її через інші засоби масової інформації, тощо. Варто зазначити, що ця технологія має подвійне практичне спрямування: технологія захисту, наприклад, для захисту від комп'ютерних вірусів і інформаційних вірусів, якими є деструктивні інформаційні впливи і технологія нападу.

Враховуючи вищенаведене можна сказати, що головною задачею інформаційної обфускації є створення алгоритмів практичного застосування різних видів інформаційно-психологічних операцій та їх можливих сполучень для представлення інформації у необхідному для сприйняття вигляді тими об'єктами інформаційного протиборства, проти яких вона і спрямована.Тому технологія проведення ІПО повинна бути скритною і непрозорою для опонента. Використання таких технологій інформаційного впливу зробить процес організації комплексного захисту інформаційних ресурсів для протилежної сторони інформаційного протиборства суттєво складнішим, оскільки процесс ведення інформаційної війни супроводжується численними неточностями и невизначеностями. З урахуванням того, що відома ціла множина механізмів проведення інформаційно-психологічних операцій, а також існує множина відомих сучасних мобільних джерел доведення інформації, які можна розглядати як джерела впливу, таких як телебачення радіомовлення, Internet, соціальні мережі, тощо., можна стверджувати, що існує ймовірність втягнення і маніпулювання у віртуальному інформаційному середовищі свідомістю великої кількості людей.

На людину яка є елементом сучасного інформаційного середовища і одночасно об'єктом інформаційного впливу, може впливати одночасно одне або декілька джерел впливу. При цьому цілі деструктивного зовнішнього впливу можуть бути як стратегічні, так і тактичні, тобто час впливу може вимірюватися від декількох днів і годин до місяців і років. Очевидно, що від урахування цих чинників залежить ефективність проведення інформаційно-психологічних операцій.

Використовуючи знання меметики, можна стверджувати, що головною задачею створення і розповсюдження мема – інформаційного повідомлення, з метою формування деструктивного інформаційного впливу, є збільшення копій створених мемів у свідомості максимально можливої кількості людей. Тут можна говорити про властивість "спадковості" мема і проводити певні аналогії з геном. Однак для повторення тих чи іншихознак гену потрібен дуже великий час який може вимірюватись сторіччями і навіть більшими відрізками часу, амему для рішення задачі "спадковості", з урахуванням можливостей сучасних інформаційних технологій, достатньо декількох годин і навіть хвилин.

Розглянемо можливі механізми впливу на людину. Відомо, що для реалізації ІПО базовими механізмами можуть бути такі: трансінформування – правдиве інформування,

псевдоінформування – напівправдиве, напівбрехливе інформування, дезінформування – суто брехливе інформування, метадезінформування – інформування при якому брехня представляється як правда у різних варіантах, мультиінформування – інформування яке реалізується за рахунок розкладу інформаційного повідомлення [3]. Базою ІПО є інформаційно-управляючі впливи які можуть представляти правдиву інформацію, брехливу інформацію, комбінацію правдивої і брехливої інформації тощо. Метою представлення у різних формах інформації, а фактично маніпуляція цією інформацією є ввід в оману людину і як наслідок маніпуляція його свідомістю, що в свою чергу дозволить привести людину як – соціальну складову СТС у потрібний стан. Фактично людина як елемент соціальної складової СТС, приводиться у стан керованого хаосу, тобто стан, який зовнішніми силами може бути змінений у потрібному напрямку з тією чи іншою ефективністю.

Розглянемо можливі моделі проведення ІПО, тобто проведення інформаційної обфускації. У разі використання одного джерела інформаційного пливу можливі варіанти коли це джерело інформації використовує різні тип ІПО. Наприклад, протягом певного часу джерело впливу представляє правдиву інформацію, через певний період цеж саме джерело відносно цих самих подій використовує інший тип ІПО – комбінацію правди і брехні, потім суцільну дезінформацію яка вже на фоні проведених раніше типів ІПО може зовсім по іншому сприйматися. Необхідно зазначити, що людина, як елемент СТС, яка підпала під дію ІПО, тобто змінила свій стан під її дією, сама може стати джерелом впливу на оточуюче соціальне середовище і викликати умовну “ соціальну ланцюгову реакцію ”зараження інформаційним вірусом, який розповсюджується у створюваних “соціоінформаційних мережах”, тобто мережах де об’єктом і суб’єктом інформаційної взаємодії є виключно людина.

Визначення 1. Соціоінформаційна мережа (СІМ) – тип мережі, в якій можуть проводитися спеціальні інформаційно-психологічні операції, як прямого (цілеспрямоване розповсюдження інформації), так і опосередкованого (хаотичне розповсюдження інформації) типу. Джерелом пливу і об’єктом на який спрямований цей вплив у СІМ є людина.

Це суттєво ускладнює практичні аспекти побудови ефективного захисту проти деструктивного інформаційного впливу і навпаки може значно підвищити ефективність проведення негативного інформаційного впливу. Оцінити цю ефективність складно, оскільки процес сприйняття людиною інформації, розповсюдження цієї інформації супроводжується багатьма невизначеностями і обмеженнями, які узагальнено можна ідентифікувати як можливості і здатності об’єктивно аналізувати інформацію. Очевидно, що таку систему “джерело впливу – об’єкт впливу ” з відповідними обмеженнями можна розглядати як систему масового обслуговування (СМО) розімкнуто-комбінованого типу. Тобто джерело формування замовлень, які ми сприймаємо як інформаційні повідомлення, знаходиться зовні об’єкта на який спрямований цей вплив і одночасно джерело впливу, яке тиражує деструктивне інформаційне повідомлення може знаходитись всередині об’єкта впливу. Виходячи з визначення 1 це може бути людина яка змінила свій початковий стан. Використовуючи теорію меметики, а також підходи запропоновані у роботі [2] будемо вважати фактом зміни стану інформаційного середовища наявність в ньому нового мема-інформаційного повідомлення. Відповідно факт наявності у інформаційному середовищі нового мема-інформаційного повідомлення будемо вважати фактом обслуговування або прийняття цього інформаційного повідомлення об’єктом на який це інформаційне повідомлення було спрямоване.

Визначення 2. Обєкт на який спрямоване деструктивне інформаційне повідомлення змінив свій стан, якщо у інформаційному просторі присутній процес змін таких повідомлень.

В теорії інформаційного протиборства не існує стандарта метрики сили впливу на інформаційний простір соціальної складової СТС [4]. В одних випадках використовують, міру змін у соціально-економічній системі після застосування інформаційного впливу [5,6]. Інші підходи визначають силу інформаційного впливу виходячи з об’єма аудиторії, кількості

відповідних публікацій, тощо [7].У даній роботі запропоновано підхід який дозволить отримати ймовірнісні моделі для оцінювання сили або ефективності проведення ІПО, враховуючи різні моделі і алгоритми їх проведення.Оцінкою ефективності є ймовірна кількість населення яке потенційно може змінити свій початковий стан.

Ефективність проведення ІПО можна оцінювати як для одного джерела впливу – одно канальна СМО, так і для декількох джерел впливу – багатоканальна СМО.

Відповідно у разі використання одного джерела впливу можна запропонувати послідовну або одноканальну модель процесу інформаційної обфускації, структурна модель якої представлена а рисунку 1.

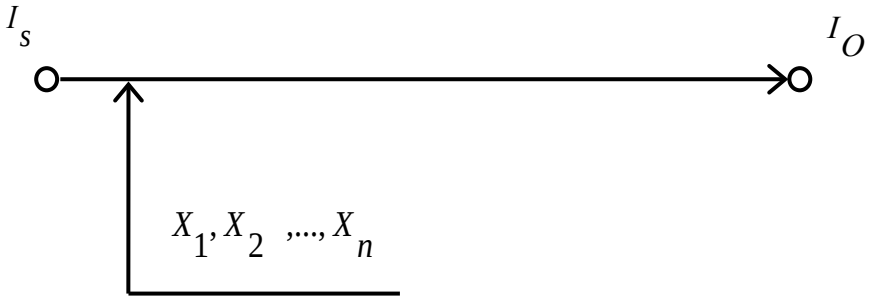

Рис.1. Структурна модель послідовної або одноканальної інформаційної обфускації

На рис. 1 представлено I_s – джерело впливу, яке використовує інформаційно-психологічний вплив типу X_1, X_2 ,..., X_n , об'єкт впливу – I_O.

Враховуючи узагальнену математичну модель для оцінювання потужності інформаційного впливу [8], яка враховує різні види джерел впливу і різні типи механізмів проведення ІПО, ймовірнісну оцінку потужності чи ефективності проведення одноканальної інформаційної обфускаціїможна представити як:

$$E_1 = P_{обсл.} \cdot V_i^j(D_m) = P_{обсл.} \cdot \sum_{i,j,m=0}^{n} (Y_m(P_j)/|D_m|) \cdot k_t , \quad (1)$$

де $P_{обсл.}$ – ймовірність присутностіінформаційногоповідомлення в інформаційному просторі, або ймовірність його обслуговування, V_i^j – показує приналежність джерела впливу до i - го класу, яке використовує j - й механізм реалізації проведення інформаційних операцій, D_m –об'єкти впливу, які розрізняються за різними категоріями ознак, $Y_m(P_j)$ – кількість об'єктів m - го класу, які змінили свій стан під дією j- го механізму впливу, k_t – коефіцієнт, який враховуєчастоту звернення до даного джерела впливу i змінюється від 0 до 1, n– відповідна кількість механізмів впливу.

Очевидно, що ефективність або іншими словами ризики наслідків проведення деструктивних інформаційних впливів визначається ймовірною кількістю об'єктів, що змінили свій стан по відношенню до початкового, тобто який був до початку проведення інформаційно-психологічних операцій.

У разі одночасного використання декількох різних джерел впливу, які можуть використовувати як різні механізми проведення ІПО так і однакові, пропонується паралельна або багатоканальна структурна модель процесу інформаційної обфускації, яка представлена на рис 2.

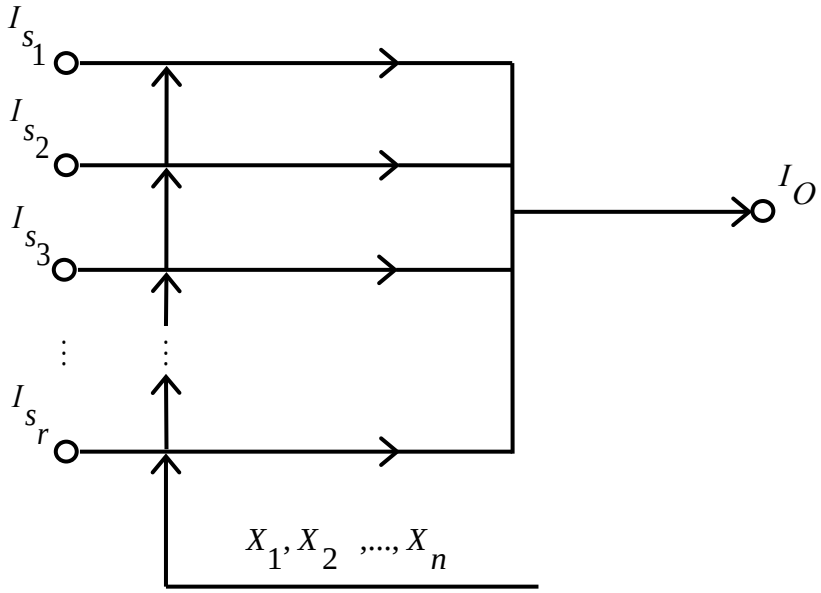

Рис 2. Структурна модель паралельної або багатоканальної інформаційної обфускації

На рисунку 2 представлено: $I_{s_1} - I_{s_r}$ – кількість джерел впливу.

При оцінюванні ефективності впливу множини мемів які одночасно знаходяться у інформаційному просторі, потрібно враховувати зв'язок між ними. Згідно роботи [9] ймовірність появи повідомлення мема - повідомлення mm_a після mm_b може бути розрахована:

$$P_t^{mm_a, mm_b} = \frac{C(mm_a, mm_b)}{C(mm_{k=a})}, \quad (2)$$

де $P_t^{mm_a, mm_b}$ – ймовірність появи мема mm_a після мема mm_b, $C(mm_a, mm_b)$ – кількість пар мемів (mm_a, mm_b), $mm_{k=a}$ – кількість копій мема mm_a.

З урахуванням виразів (1) і (2) ефективність багатоканальної обфускації може бути представлена як:

$$E_r = P_t^{mm_a, mm_b} \cdot \sum_{i,j,m=0}^{n} (Y_m(P_j)/|D_m|) \cdot k_t =$$

$$= \frac{C(mm_a, mm_b)}{C(mm_{k=a})} \cdot \sum_{i,j,m=0}^{n} (Y_m(P_j)/|D_m|) \cdot k_t$$

Отримані вирази і дозволяють отримати поточну або статичну оцінку ефективності проведення інформаційно-психологічних операцій. Для рішення задачі прогнозування щодо ризиків проведення інформаційної обфускації необхідно враховувати інтенсивність або іншими словами закони розподілу випадкових подій – виникнення інформаційних повідомлень - мемів у інформаційному просторі.

Практична реалізація

Продовження дослідження даного питання полягає у реалізації програмного забезпечення яке дозволить проводити оцінювання ефективності проведення інформаційної

обфускації у реальному часі. Узагальнений алгоритм процесу оцінювання передбачає виконання таких дій:

1. Аналіз контенту потенційних джерел впливу на наявність спеціальних інформаційних повідомлень (тематика, кількість копій однакових мем - повідомлень у різних джерелах, кількість різних мем - повідомлень, але спрямованих на одну тематику).
2. Аналіз типу джерел впливу та механізмів проведення ІПО.
3. Оцінювання поточних ризиків проведення ІПО для різних категорій населення
4. (доступ до одного джерела впливу або доступ до декількох джерел впливу).
5. Рішення задачі прогнозування щодо ризиків проведення ІПО.

Представлені результати отримані в ході виконання державної науково - дослідної теми 51-Д-375 “Методологія комплексного захисту інформації в соціотехнічних системах в умовах інформаційної війни”.

Висновки

Представлені результати можуть бути використані у процесі ведення інформаційного протиборства, а саме оцінюванні ефективності проведення спеціальних інформаційно-психологічних операцій проти соціальної складової СТС, з урахуванням типів джерел впливу та механізмів проведення ІПО. Це у свою чергу дозволить організувати ефективний захист від деструктивних інформаційних впливів, а також реалізувати запропонований підхід щодо комплексного захисту інформаційних ресурсів на рівні управління інформаційною безпекою – “підприємство-регіон-держава”.

Література

1. Цыганов В.В. Информационноеуправлениесамоорганизациейсетевых структур /В.В. Цыганов // Информационныевойны. – 2015. – № 3. – С. 2-10.

2.Артёмов А.А. Теоретические основы информационного управления / А.А. Артёмов // Информационныевойны. – 2015. – № 3. –С. 83-97.

3.Остапенко Г.А. Информационные операции иатаки в социотехнических системах / Г.А. Остапенко. – М.: Горячая линия – Телеком, 2007. – 134 с.

4. Макаренко С.И.Терминологический базис в области нформационного противоборства /С.И. Макаренко, И.Л. Чукляев // Вопросы кибербезопасности.– 2014. –№1(2).– С.13-21.

5. Расторгуев С.П. Философия информационной войны / С.П. Расторгуев. – М.: Аутоплан, 2000. – 444 с.

6. Bespalova B.P., Fedorov A.V. The role of the mass media in changing public opinion. Using the mass media as an ideological weapon //The Russian Academic journal,Vol. 23, Issue 1, 2014, pp. 0-0

7. Bazan S. B., Saad S., Tesfa A. Infowar on the web: measuring mass annoyance Proceedings of the 2014 ACM conference on Web science. – ACM, 2014. – pp. 283-284.

8. Дудатьєв А.В. Модлі для організації протидіїінформаційним атакам / А.В. Дудатьєв // Захист інформації. – 2015. – № 2. – С.157-162.

9. Simmons M. P., Adamic L. A., Adar E. Memes Online: Extracted, Subtracted, Injected, and Recollected //ICWSM. – 2011. – Т. 11. – pp.17-21.

Надійшла 25.10.2015 р. Рецензент: д.т.н., проф. Барабаш О.В.