Олійников Роман Васильович, доктор техічних наук, Начальник відділу наукових досліджень Приватного акціонерного товариства «Інститут інформаційних технологій».
E-mail: ROliynykov@gmail.com.
Олейников Роман Васильевич, доктор технических наук, начальник отдела научных исследований закрытого акционерного общества «Институт информационных технологий».
Oliynykov Roman, doctor of technical sciences, head of scientific research department of joint-stock company «Institute of information technologies».

Горбенко Іван Дмитрович, доктор техічних наук, Головний конструктор Приватного акціонерного товариства «Інститут інформаційних технологій».
E-mail: GorbenkoI@iit.kharkov.ua.
Горбенко Иван Дмитриевич, доктор технических наук, главный конструктор закрытого акционерного общества «Институт информационных технологий».
Gorbenko Ivan, doctor of technical sciences, chief designer of joint-stock company «Institute of information technologies».

Казимиров Олександр Володимирович, кандидат технічних наук, Технічний тест-аналітик у компанії EVRY Norge AS.
E-mail: okazymyrov@gmail.com.
Казимиров Александр Владимирович, кандидат технических наук, технический тест-аналитик в компании EVRY Norge AS.
Kazymyrov Oleksandr, candidate of technical sciences, Technical Test Analyst in the company EVRY Norge AS.

Руженцев Віктор Ігорович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Харківського національного університета радіоелектроніки.
E-mail: vityazik@rambler.ru.
Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники.
Ruzhentsev Victor, candidate of technical sciences, Assossiate Professor of The Department of Information Technology Security, Kharkiv National University of Radio Electronics.

Горбенко Юрій Іванович, кандидат технічних наук, технічний директор Приватного акціонерного товариства «Інститут інформаційних технологій».
E-mail: GorbenkoU@iit.kharkov.ua.
Горбенко Юрий Иванович, кандидадт технических наук, технический директор закрытого акционерного общества «Институт информационных технологий».
Gorbenko Iurii, candidate of technical sciences, technical director of joint-stock company «Institute of information technologies».

УДК 004.056

МОДЕЛІ ДЛЯ ОРГАНІЗАЦІЇ ПРОТИДІЇ ІНФОРМАЦІЙНИМ АТАКАМ

Андрій Дудатьєв

Поняття інформаційної безпеки доцільно розглядати з позиції оцінювання та забезпечення комплексної інформаційної безпеки в умовах ведення інформаційної війни. Фактично констатується необхідність урахування специфіки технологій проведення спеціальних інформаційних операцій з боку об'єкта впливу на етапах проектування, впровадження і супроводу комплексних систем захисту інформації. Досвід останніх років і подій показує, що ефективність застосування інформаційної зброї у сучасних умовах інформатизації суспільства достатньо велика і за своїми кількісними показниками може бути порівняна зі зброєю масового знищення. У статті представлені дві математичні моделі, які дозволяють оцінити потужність інформаційного впливу з урахуванням специфіки джерела та механізму реалізації впливу, а також запропонувати управлінські рішення для підготовки і подальшого проведення спеціальних інформаційних контроперацій. Аналіз запропонованих моделей дозволив сформулювати узагальнені етапи методики для прийняття ефективних рішень щодо управління інформаційною безпекою на об'єкті захисту в умовах інформаційної війни.
Ключові слова: *інформаційна війна, інформаційна зброя, інформаційно-психологічний вплив, комплексна система захисту інформації.*

Вступ. Моделювання інформаційної взаємодії двох або більшої кількості суб'єктів за умови їхньої життєдіяльності в умовах інформаційної війни зводиться до розробки математичних моделей інформаційного протиборства. При цьому якість розроблених моделей визначається ґрунтовністю теоретичних розробок і адекватним математичним апаратом. Конкуруючі об'єкти у більшості випадків практикують проведення інформаційних операцій для боротьби за різноманітні

ресурси, вирішуючи при цьому свої геополітичні задачі, соціальні, економічні проблеми тощо. Суттєво активізується і поширюється процес ведення інформаційних війн за «мозок людини», їхню свідомість, відношення до життя, суспільства, середовища, у якому здійснюється життєдіяльність. Оскільки негативний інформаційний вплив ініціює виникнення нових або загибель старих соціотехнічних систем (СТС), то головною метою інформаційних війн є запуск або генерація спеціальних програм самоусунення, самообмеження будь-якої СТС, здатної до самонавчання і адаптації до внутрішніх і зовнішніх впливів. Для реалізації цієї мети потрібні різні і потужні ресурси, одним з головних яких є час. Зрозуміло, що чим менший час і чим більша кількість елементів СТС охоплена спеціальною інформаційною операцією, тим вона ефективніша.

При проведенні інформаційної війни конкуруючі сторони проводять боротьбу і за володіння інформаційною зброєю. За визначенням інформаційна зброя представляє собою засоби, що застосовуються для активізації, знищення, блокування або створення в інформаційній системі процесів, у яких зацікавлений суб'єкт, що застосовує зброю. Оскільки застосування інформаційної зброї передбачає можливість використання декількох механізмів, то зрозуміло, що і захист від цього впливу має бути комплексним.

Актуальність. Перефразувавши відому фразу: «Необхідно захищати власні інформаційні ресурси і захищатися від інформаційного впливу», можна сказати так: «Необхідно комплексно захищати власні інформаційні ресурси і комплексно захищатись від інформаційного впливу», оскільки ризики від інформаційного впливу можуть бути суттєвими і навіть критичними для об'єктів всіх рівнів управління. Тому інформаційну безпеку доцільно розглядати з позиції комплексної інформаційної безпеки сучасних соціотехнічних систем, які функціонують в умовах інформаційної війни та їх життєдіяльність супроводжується різного роду аваріями і катастрофами, зростаючими потребами у використанні енергії різного походження, погіршенням стану екології, проведенням терористичних актів. Все це визначає актуальність розробки математичних моделей ймовірних варіантів проведення інформаційних війн.

Аналіз існуючих досліджень. Проблемі дослідження технологій ведення інформаційних війн присвячені дослідження багатьох закордонних і вітчизняних вчених [1, 2, 4]. У наведених роботах розглянуто достатньо широке коло проблем і задач, пов'язаних з загальною концепцією державної інформаційної політики в умовах можливого використання множини засобів і заходів ведення інформаційної війни, представлені теоретичні аспекти і наукові основи інформаційної безпеки СТС.

Разом із тим існує комплексна проблема, що полягає у вирішенні двоєдиної задачі, яка на поточний час недостатньо формалізована: оцінювання потужності або ефективності джерел впливу з використанням відповідних інформаційно-психологічних впливів; оцінювання ймовірнісних значень можливості виникнення "небажаних" подій на об'єкті захисту і їх рангів.

Метою даної роботи є подальший розвиток загальної теорії комплексної інформаційної безпеки соціотехнічних систем, що дозволить практично реалізувати ефективні технології і механізми захисту і забезпечити достатній рівень захищеності в умовах інформаційної війни.

Для досягнення мети дослідження сформульовані такі *задачі:*

1. Провести аналіз умов функціонування соціотехнічних систем.

2. Розробити математичні моделі для оцінювання ефективності спеціальних інформаційних операцій об'єктами впливу, а також для реалізації ефективної протидії спеціальним інформаційним операціям.

Модель для оцінювання ефективності джерела впливу. Соціотехнічна система функціонує у сучасному інформаційному середовищі, ознаки якого наведені у [2]. Логіка розвитку СТС, її соціальної та технічної частин говорить про те, що зовнішні штучні процеси зміни інформаційного середовища, які проходять з великою інтенсивністю, можуть привести до того, що швидкість зміни середовища буде відбуватися значно швидше, ніж зміни СТС. Як наслідок, це може привести до виникнення інформаційного ураження.

Відомі три основні механізми проведення спеціальних інформаційних операцій: механізми реалізації пропаганди, агітації та інформаційного протиборства. Відповідно для можливих станів об'єктів інформаційної взаємодії (активний-пасивний) потрібно використовувати найбільш ефективні механізми проведення спеціальних інформаційних операцій [3]. Інформаційна операція є складовою так званих гібридних війн і її наявність є ознакою виникнення і проявлення ймовірних так званих економічних війн або військових загроз. Технологій проведення інформаційних операцій достатньо багато. Наприклад, інформаційна зброя, яка використовується у се-

редовищі Internet, отримує розвиток за такими напрямами: розвідка, проведення спеціальних операцій, планування інформаційних операцій, управління їх проведенням та оцінка їх ефективності [2]. Створення та розвиток інформаційної зброї супроводжується розробкою відповідних технічних засобів і інформаційних технологій. Основою реалізації механізмів активного впливу на соціальну складову СТС і ведення спеціальних інформаційних операцій є такі інформаційно-психологічні впливи [4]:

- трансінформування;
- псевдоінформування;
- дезінформування;
- мультиінформування.

Коли інформаційна зброя використовується тільки одним з протидіючих опонентів (суб'єкт активний), то зрозуміло, що стан іншого суб'єкта (пасивного) в більшості випадків є приреченим. Саме тому розробка математичної моделі проведення інформаційної війни повинна враховувати можливості опонентів використовувати різні джерела впливу та ті чи інші механізми реалізації інформаційного впливу. Для ідентифікації ймовірних джерел впливу та об'єктно-суб'єктних моделей взаємодії введемо такі позначення:

V_i – різні джерела впливу, які використовують відповідні механізми застосування інформаційного впливу, наприклад, Internet, телебачення, друковані ЗМІ;

D_m – об'єкти впливу, які доцільно розрізняти за різними критеріями, наприклад, соціальні об'єкти, технічні об'єкти тощо;

Y_m – кількість об'єктів, які змінили свій стан під впливом інформаційного впливу P_j.

Враховуючи принцип адитивності, можна запропонувати таке співвідношення для оцінювання ефективності інформаційного впливу:

$$V_i(D_m) = Y_m(P_j) / |D_m|, \qquad (1)$$

де $|D_m|$ – потужність множини D_m.

З урахуванням того, що одне джерело впливу може одночасно застосовувати декілька механізмів реалізації інформаційного впливу відносно одного об'єкта впливу, використовуючи такі дії, як: дискредитація, агітація, недобросовісна конкуренція тощо. Аналітичний вираз для оцінювання потужності інформаційного впливу можна представити як узагальнену математичну модель, що враховує вищеозначені особливості впливу

$$V_i^j(D_m) = \sum_{i,j,m=1}^{n} (Y_m(P_j) / |D_m|) \cdot k_t, \qquad (2)$$

де V_j^i показує приналежність джерела впливу до *i*-го класу, яке використовує *j*-й механізм реалізації інформаційних операцій, $Y_m(P_j)$ – кількість об'єктів *m*-го класу, які змінили свій стан під дією *j*-го механізму впливу, k_t – коефіцієнт, який враховує частоту звернення до даного джерела впливу *i* змінюється від 0 до 1, *n* – відповідна кількість класів та механізмів впливу.

Очевидно, що ефективність інформаційного впливу визначається кількістю об'єктів, що змінили свій стан у тому напрямку, який необхідно для об'єкта впливу. Аналіз виразу (2) дає можливість зробити попередній аналіз ризиків відносно ефективності джерел та відповідних механізмів проведення спеціальних інформаційних операцій, які використовує об'єкт впливу і проведення попереднього ранжування відносно потужності ймовірних інформаційних спеціальних операцій. Але для прийняття рішення щодо побудови ефективного комплексного захисту від проведення спеціальних інформаційних операцій потрібно визначення найменш захищених місць і елементів, причин і ймовірних наслідків проведення спеціальних інформаційних операцій.

Модель для реалізації протидії інформаційним впливам з боку супротивника. Ефективність захисту і протидії інформаційним операціям залежить, в свою чергу, від виконання проведення спеціальних операцій, таких як: розвідки відносно можливості проведення спеціальних інформаційних операцій з боку потенційного супротивника; своєчасне виявлення початку проведення інформаційної атаки та її інформаційно-аналітичний супровід; ефективна протидія інформаційній атаці. Для реалізації ефективності протидії інформаційним операціям пропонується логіко-ймовірнісна модель, яка для наочності розроблена у вигляді дерева-подій і представлена на рис. 1. Ця модель фактично формалізує поточний стан об'єкта захисту і представляє процес проведення пропаганди з боку об'єкта впливу, який використовує різні механізми проведення інформаційно-психологічного впливу, такі як: трансінформування, псевдоінформування, дезінформування. В якості базових подій представлені початкові події, які можуть бути причинами ефективного проведення спеціальних інформаційних операцій. Результатами моделювання будуть ймовірнісні характеристики всіх подій, які потенційно можуть виникнути на досліджуваному об'єкті та їх наслідків, а також ранги цих подій. Це надасть можливість мінімізувати можливі втрати, побудувати ефективний комплексний

захист від інформаційного впливу для об'єкта захисту шляхом використання оптимального складу засобів та заходів. Методологія дослідження логіко-ймовірнісної моделі представлена у [5].

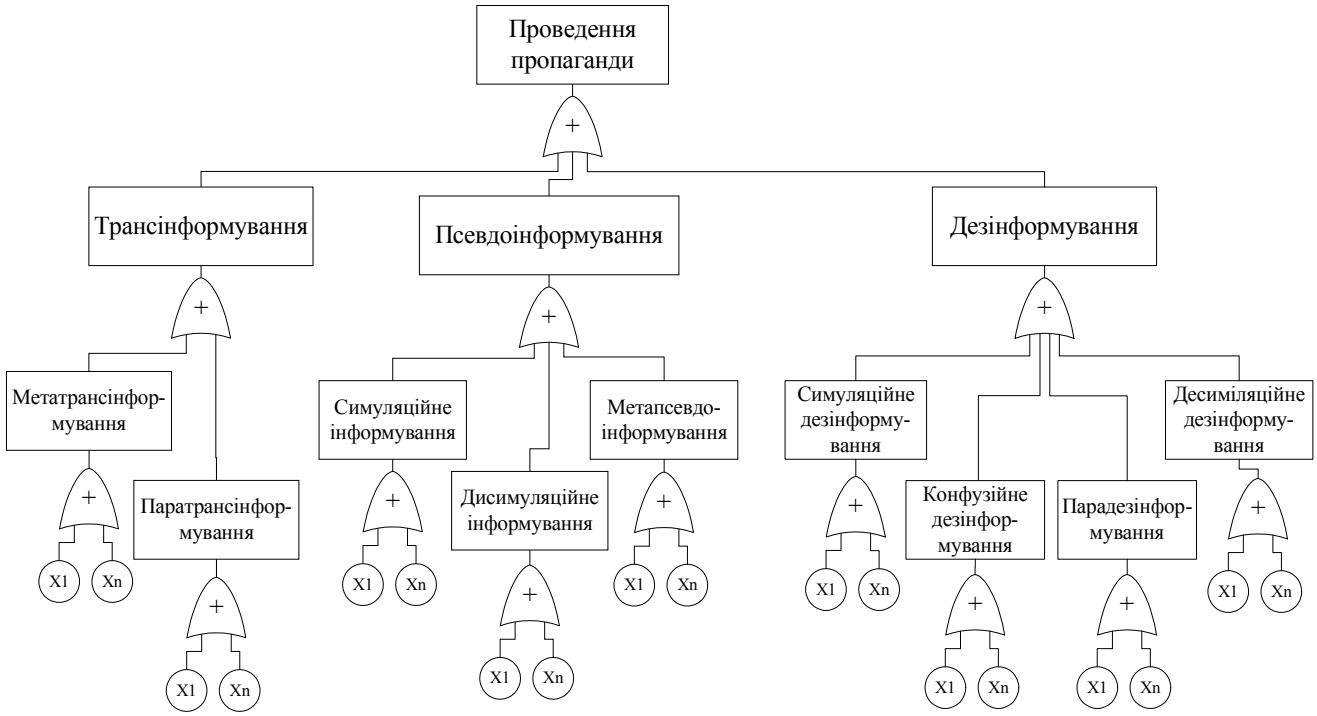

Рис. 1. Логіко-ймовірнісна модель для оцінювання ймовірності проведення пропаганди

В якості базових подій $X_1 - X_2$ розглядаються такі події, які потенційно можуть відбутися в системі, або події, характерні для системи. Наприклад, X_1 – відсутня спеціальна служба моніторингу інформаційного простору (ІАС), X_2 – відсутня або недостатня нормативно-правова база щодо заборони певних ЗМІ, X_3 – наявність інсайдерів, X_4 – наявність зовнішніх «зацікавлених структур».

У практичній площині результати моделювання дозволяють нам вирішити такі задачі:

1. Визначити найбільш ефективні або небезпечні джерела проведення інформаційних операцій, а також використовуваних механізмів з боку об'єкта впливу;

2. Визначити причинно-наслідковий зв'язок ефективності проведення інформаційних операцій з боку об'єкта впливу;

3. Запропонувати комплексний захист у вигляді проведення спеціальних контроперацій.

Розроблені моделі і вирішення наведених 3-х задач дозволяє запропонувати методику для прийняття управлінських рішень щодо керування інформаційною безпекою на об'єкті захисту в умовах інформаційної війни. Доцільно розглядати процес управління інформаційною безпекою як неперервний і багаторівневий, тому суть методики має враховувати принципи неперервності і багаторівневості. З урахуванням внутрішньої інформаційної інфраструктури та побудови більшості об'єктів захисту, зокрема держави як об'єкта захисту та специфіки зовнішнього і внутрішнього інформаційного середовища методику доцільно розробляти на рівні «підприємство-регіон-держава». Для ефективної інформаційної протидії необхідно побудувати відповідну ефективну організацію, яка б структурно і функціонально відповідала і вирішувала вище наведені задачі.

Успішна практична реалізація методики передбачає наявність відповідних структур, таких як служба інформаційної безпеки підприємства або інформаційно-аналітичні центри на рівні регіонадержави до компетенції яких і відноситься вирішення відповідних задач на своєму рівні прийняття рішення. Також необхідна наявність спеціального інформаційно-технологічного забезпечення у вигляді спеціальних технічних і програмних засобів, а також організаційних заходів для рішення вищенаведених задач.

Базові узагальнені етапи уніфікованої методики протидії інформаційним впливам такі:

1. Проведення постійного моніторингу зовнішнього і внутрішнього інформаційних середовищ на предмет виявлення можливості проведення спеціальних інформаційних операцій.

2. Планування інформаційних контроперацій.

3. Управління процесом проведення контроперацій та оцінювання їх ефективності.

Приклад використання запропонованих моделей. Дослідження розроблених моделей пропонується виконувати у два етапи: 1-й етап – проведення аналізу зовнішнього і внутрішнього інформаційного середовища з точки зору можливості та ефективності використання різних джерел впливу, а також різних механізмів проведення інформаційних операцій. 2-й етап – проведення аналізу зовнішнього і внутрішнього інформаційного середовища, а також загальної інфраструктури об'єкта захисту з метою виявлення множин загроз і вразливостей, причин їх виникнення і визначення наслідків інформаційного ураження. Для прикладу наведемо таку узагальнену постановку задачі.

Заплановано проведення спеціальних інформаційних операцій на території, на якій постійно проживає N людей. Для реалізації інформаційних операцій використовуються 2 джерела доведення інформації до населення: ресурси глобальної мережі Internet і телебачення. Спеціально проведені дослідження показують, що послугами мережі Internet користуються приблизно N_1% населення, а послуги телебачення отримують N_2% населення. При цьому певна кількість населення одночасно отримує інформацію з двох джерел – Internet і телебачення. Необхідно визначити ефективність ймовірного застосування різних джерел впливу з використанням різних механізмів проведення інформаційних операцій.

1–етап. Попередній аналіз інформаційного середовища показав, що в середовищі мережі Internet використовується механізм пропаганди, а в телебаченні механізм агітації. Припустимо, що послугами Internet користуються N_1 осіб, які потенційно можуть змінити свою початкову позицію. У такому випадку логічно припустити, що механізм телевізійної пропаганди спрямований на $N - N_1 = N_2$ кількість суб'єктів.

2. Згідно статистики, середня кількість абонентів Internet у регіонах України складає приблизно 20% населення, а послугами телебачення користуються приблизно 95% населення [6].

Для чисельного експерименту наведемо такі значення: населення регіону складає $N = 800000$ осіб, відповідно потенційна кількість користувачів складає $N_1 = 1600000$, а кількість населення, яка користується телебаченням складає $N_2 = 6400000$. Коефіцієнт k_t показує тривалість впливу або частоту використання того чи іншого джерела впливу. Коефіцієнт може змінюватись від 0 до 1. Якщо k_t наближений до 0, то тривалість незначна, і навпаки, якщо k_t наближений до 1, то тривалість або частота впливу максимальна. Для розрахунків приймемо значення k_t =0,2 для Internet і k_t =0,5 для телебачення. Необхідно врахувати, що є користувачі, які отримують одночасно послуги як Internet, так і телебачення. Приймаємо, що ця частка населення складає також 20%, але від значення N_2, тобто 1280000 осіб. Для проведення розрахунку використаємо вираз (2), а результат розрахунку, проведеного із запропонованими даними, представлений на рис. 2.

З діаграми видно, що найбільшу потенційну небезпеку, як джерела ураження, представляє телебачення з використанням механізму агітації, але особливу увагу слід звернути на сектор діаграми, який перекривається двома джерелами впливу, як Internet, так і телебаченням. Такий сектор пропонується назвати *сектором ймовірного стійкого ураження.* Також варто звернути увагу на сектор, який відображає умовну групу населення «інші», яка не підпадає під досліджувані джерела впливу і боротьба цю групу має бути попереду.

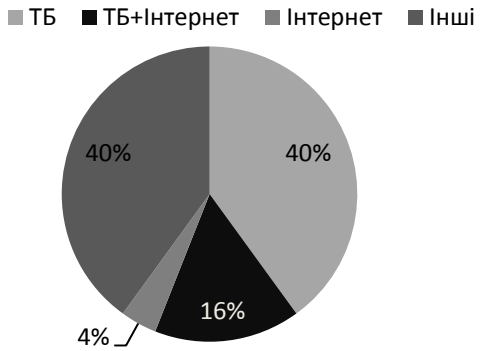

Рис. 2. Графічна інтерпретація результатів інформаційного ураження населення

3–етап. Аналіз логіко-ймовірнісної моделі і проведення розрахунку дозволить отримати ймовірнісні характеристики всіх подій, що враховані у моделі, а також отримати їх ранги, що дозволить перейти до етапу підготовки рішень щодо протидії інформаційним впливам, вибору оптимального рішення і виконанню послідовного постійного контролю над рівнем інформаційної безпеки.

Висновки. Реальне існування технологій ведення інформаційних війн вимагає наявності спеціальних моделей, методів і методик для реалізації ефективної протидії або захисту від негативного інформаційного впливу. У статті запропоновано дві моделі, які дозволяють оцінити потужність інформаційного впливу з урахуванням

специфіки джерела та механізму реалізації впливу, а також запропонувати управлінські рішення для підготовки і подальшого проведення спеціальних інформаційних контроперацій.

ЛІТЕРАТУРА

[1]. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны /А.В. Манойло, Петренко А.И., Фролов Д.Б. – М.: Горячая линия – Телеком, 2003. – 541с.

[2]. Расторгуев В.П., Литвиненко М.В. Информационніе операции в сети Интернет / В.П. Расторгуев, М.В. Литвиненко – М.: АНО ЦСоиП, 2014. – 128 с.

[3]. Дудатьєв А.В. Теоретичні аспекти та технології керованого хаосу для реалізації комплексного інформаційного захисту соціотехнічних систем, Інформаційні технології та комп'ютерна інженерія. – 2014. – № 2(30). – С.28-32.

[4]. Остапенко Г.А. Информационные операции и атаки в социотехнических системах / Г.А. Остапенко – М.: Горячая линия – Телеком, 2007. – 134 с.

[5]. Дудатьєв А.В. Розробка уніфікованих моделей системного проектування оптимальних систем захисту інформаційних ресурсів / А.В. Дудатьєв // Вісник Черкаського технологічного університету. – 2008. – №1. – С. 3-8.

[6]. http://podrobnosni.ua922673-kolichestvo-internet-polzovatelej-v-ukraine

REFERENCES

[1]. AV Manoilo State-owned ynformatsyon-Nye politics in the information and conditions psyholohycheskoy /A.V war. Manoilo, PET-Rank AI, Frolov DB - M .: hotline, Telecom, 2003, 541 p.

[2]. Rastorguev VP, Litvinenko MV Ynformatsy-onnie operations in the network Internet / VP Rastorhuev, NV Litvinenko - M: AIE TsSoyP, 2014, 128 p.

[3]. AV Dudatyev Theoretical aspects and technology controlled chaos to implement a comprehensive information security socio-technical systems, IT and computer inzhe-Neri, 2014, № 2 (30), P.28-32.

[4]. Ostapenko GA Clearing operations and attacks in sotsyotehnycheskyh systems / GA Ostapenko, M.: hotline, Telecom, 2007, 134 p.

[5]. AV Dudatyev Development of standardized models of optimal system design of protection of information resources / AV Dudatyev // Bulletin of Cherkassy University of Technology-theta, 2008, №1,P. 3-8.

[6]. http: //podrobnosni.ua922673-kolichestvo-internet-polzovatelej-v-ukraine

МОДЕЛИ ДЛЯ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННЫМ АТАКАМ

Понятие информационной безопасности целесообразно рассматривать с позиции оценки и обеспечения комплексной информационной безопасности в условиях ведения информационной войны. Фактически констатируется необходимость учета специфики технологий проведения специальных информационных операций со стороны объекта воздействия на этапах проектирования, внедрения и сопровождения комплексных систем защиты информации. Опыт последних лет и событий показывает, что эффективность применения информационного оружия в современных условиях информатизации общества достаточно велика и по своим количественным показателям может быть сравнима с оружием массового уничтожения. В статье представлены две математические модели, которые позволяют оценить мощность информационного воздействия с учетом специфики источника и механизма реализации воздействия, а также предложить управленческие решения для подготовки и последующего проведения специальных информационных контроперацій. Анализ предлагаемых моделей позволил сформулировать обобщенные этапы методики для принятия эффективных решений по управлению информационной безопасностью на объекте защиты в условиях информационной войны.

Ключевые слова: информационная война, информационное оружие, информационно-психологическое воздействие, комплексная система защиты информации.

MODELS TO COUNTER INFORMATION ATTACKS

The concept of information security should be considered from the complex information security evaluating and providing in an information warfare point of view. In fact, the need for special information operations performing specific technologies are stated during complex information security systems design, implementation and maintenance. The experience of recent years and events shows that the information weapon usage effectiveness in modern conditions of society informatization is tremendous and their quantitative indicators can be compared to the weapon of the mass destruction. Two mathematical models are presented to assess information influence power considering source peculiarities and to propose management solutions for training and further special information counteractions implementations. Analysis of the proposed models allowed to formulate generalized stages of the technique for effective management solutions for information security at the facility protection in the information war.

Index terms: information warfare, information weapons, information and psychological impact, integrated system of information.

Дудатьєв Андрій Веніамінович, кандидат технічних наук, докторант, доцент кафедри захисту інформації, Вінницький національний технічний університет.
E-mail: andreysaf60@mail.ru.

Дудатьев Андрей Вениаминович, кандидат технических наук, доцент кафедры защиты информации, Винницкий национальный технический университет.

Dudatyev Andrew, PhD, Associate Professor of Information security Academic Department, Vinnytsia National Technical University.