Міністерство освіти і науки України
Вінницький національний технічний університет

А. В. Дудатьєв

КОМПЛЕКСНА ІНФОРМАЦІЙНА БЕЗПЕКА СОЦІОТЕХНІЧНИХ СИСТЕМ: МОДЕЛІ ВПЛИВУ ТА ЗАХИСТУ

Монографія

Вінниця
ВНТУ
2017

УДК 007.51:004.5
Д81

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 1 від 30.08.2017 р.)

Рецензенти:
В. Л. Бурячок, доктор технічних наук, професор
О. Є. Архіпов, доктор технічних наук, професор

Дудатьєв, А. В.

Д81 Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту : монографія / А. В. Дудатьєв. – Вінниця : ВНТУ, 2017. – 128 с.

ISBN 978-966-641-711-7

В монографії розглянуто питання комплексної інформаційної безпеки соціотехнічних систем. Запропоновано аксіоматику теорії інформаційної взаємодії типу «об'єкт–суб'єкт» та класифікацію інформаційних вірусів, що можуть бути використані для «інфікування» соціальної частини соціотехнічної системи. Представлено модель інформаційного впливу та моделі і методи протидії спеціальним кібернетичним операціям.

Запропоновано модель інформаційної підтримки та структурну модель багаторівневого інформаційно-аналітичного центру управління комплексною інформаційною безпекою

УДК 007.51:004.5

ISBN 978-966-641-711-7

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ДА – детермінований автомат
ІВ – інформаційна війна
ІАЦ – інформаційно-аналітичний центр
ІзОД – інформації з обмеженим доступом
ІКО – інформаційно-кібернетична операція
ІКТ – інформаційно-комунікаційні технологології
ІМ – інформаційний мем
ІПО – інформаційно-психологічна операція
НДА – недетермінований автомат
ОВ – об’єкт впливу
ПІБ – політика інформаційної безпеки
ППР – підготовка і прийняття рішень
СІМ – соціоінформаційна мережа
СІО – спеціальні інформаційні операції
СТС – соціотехнічна система
СЦ – ситуаційний центр
ЦВ – центр впливу
FC – ([Flexible]C[ombined]) – метод управління комплексною інформаційною безпекою соціотехнічних систем

ВСТУП

XXI сторіччя ознаменувало бурхливий розвиток у сфері інформаційно-комунікаційних технологій (ІКТ), за рахунок чого суттєво підвищились можливості людства щодо обміну інформацією, спілкування «без кордонів», створення різноманітних «груп за інтересами» у соціальних мережах тощо. Здобутки технічного прогресу дозволили сформувати нові поняття – інформаційне суспільство та кібернетичний простір, які у процесах інформаційної, технічної, соціальної, економічної взаємодії можуть виступати у ролі суб'єкта або об'єкта інформаційних відносин. Однак, крім позитивних результатів, розвиток ІКТ призвів до глобальних проблем, які пов'язані, в першу чергу, зі забезпеченням комплексної інформаційної та кібернетичної безпеки. Комплексна інформаційна безпека у даному випадку полягає у реалізації захисту безпосередньо інформаційних ресурсів, технологічного обладнання, інших ресурсів та захисту соціуму від проведення кібернетичних атак або спеціальних інформаційних операцій (СІО), які, у свою чергу, можуть бути спрямовані на технічну або соціальну частину соціотехнічної системи (СТС).

СІО – це технологія проведення сучасної інформаційної війни, яка є складовою, так званої, гібридної війни. Метою проведення інформаційної війни є перепрограмування свідомості людини або групи людей. Подальше використання такого соціуму дозволить його використовувати як внутрішнє джерело інформаційного впливу на інші елементи соціуму з подальшим формуванням і поширенням потрібних думок і проведення необхідних дій, що можуть бути реалізовані, у тому числі у вигляді деструктивного впливу на технічну складову СТС.

Термін «інформаційна війна» вперше зустрічається у 1976 році. Томас Рона використав термін «інформаційна війна» у звіті, який він підготував для компанії Boeing під назвою «Системи озброєння і інформаційна війна» [1]. Т. Рона вказав, що інформаційна інфраструктура є ключовим компонентом американської економіки. В той самий час вона стає вразливою ціллю як у воєнний, так і у мирний час. До того часу було сформовано повне розуміння того, що інформація може бути як ціллю, так і зброєю. Офіційно цей термін був введений в директиві міністра оборони США DODD 3600 від 21 грудня 1992 року.

Використання сучасних кібернетичних систем управління у важливих галузях народного господарства, наприклад, військовій, енергетичній, транспортній, економічній діяльності створює нові вразливі місця для держави, якими можуть скористатися різні потенційні суб'єкти деструктивного впливу. Сучасна кібернетична атака передбачає широкий набір дій: псування веб-сайтів, порушення цілісності, конфіденційності і доступності інформації, інфікування свідомості людини, ініціювання за рахунок дій «інфікованої» людини або спеціального шкідливого програмного забезпечення, відмови технологічного обладнання тощо. Можливості для проведення деструктивної діяльності в кіберпросторі доволі широкі – такі, що при відносно невеликих ресурсах проведення масштабної кібератаки може дозволити собі відносно невелика держава. Прикладом може служити північна Корея, з території якої був розповсюджений вірус WannaCray, який атакував тисячі комп’ютерів по всьому світу і завдав великої шкоди, або ефективне використання віруса групи StuxNet, що дозволило зробити Іран більш поступливим щодо своєї ядерної програми.

Україна як держава протягом останніх років проводить достатньо велику роботу щодо захисту свого інформаційного та кіберпростору.

Нормативно-правова база держави в цій сфері постійно розширюється. У 2005 році була ратифікована Конвенція Ради Європи про кіберзлочинність. Згодом прийнято низку законів та спеціальних постанов Кабінету Міністрів України та РНБО, які дозволяють поступово будувати захищену інфраструктуру держави. Так, у 2011 році, відповідно до Указу Президента України «Про виклики та загрози національній безпеці України у 2011 році» ухвалено рішення про створення Єдиної загальнодержавної системи протидії кіберзлочинності. З огляду на важливість і критичність питань безпеки на рівні держави 25 січня 2015 року Президент України Петро Порошенко ввів у дію рішення РНБО про створення та забезпечення діяльності Головного ситуаційного центру України до якого надходитиме від державних служб і правлінь інформація з обмеженим доступом. Згідно з рішенням РНБО Головний ситуаційний центр функціонуватиме як програмно-апаратний комплекс зі збору, накопичення й обробки інформації, необхідної для підготовки та прийняття рішень у сфері національної безпеки і оборони [2]. Оскільки інформаційна безпека та кібербезпека

є важливою складовою національної безпеки, то її гарантоване забезпечення має бути невід'ємною частиною реалізації рішення РНБО.

Однак, незважаючи на відповідне технічне і нормативно-правове забезпечення, реалізувати ефективний комплексний захист СТС доволі складно, оскільки проведення СІО передбачає використання людини з її психологічними особливостями, що накладає певні труднощі. Саме на вирішення питань щодо формалізації та систематизації моделей та методів проведення деструктивних інформаційних впливів, направлених на соціальну частину СТС, і методів захисту від них спрямована представлена робота.

Автор висловлює щиру подяку зав. кафедри ЗІ (Вінницький національний технічний університет) д. т. н., проф. В. А. Лужецькому за слушні зауваження та поради, що дало можливість покращити представлену роботу, а також рецензентам зав. кафедри інформаційної безпеки (Державний університет телекомунікацій) д. т. н., професору В. Л. Бурячку і д. т. н., проф. О. Є. Архіпову (НТУУ «КПІ» ім. І. Сікорського), обговорення з якими сприяло більш чіткому і зрозумілому викладенню матеріалу.

1 ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СОЦІОТЕХНІЧНИХ СИСТЕМ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

1.1 Інформаційний та кібернетичний простори – середовище проведення спеціальних інформаційних операцій

Методи інформаційної війни використовувались в глибоку давнину при веденні численних війн. Дезінформування, проведення пропаганди з метою дезорієнтації як війська, так і населення країни-супротивника використовувалось з метою формування необхідної інформаційної моделі. Сучасні технології ведення інформаційної війни, які базуються на різних методах маніпулювання інформацією, використовують можливості сучасних інформаційного та кіберпростору. Ці можливості обумовлюються, в першу чергу, можливостями створеннями системи зв’язків між користувачами та різними об’єктами, що входять у глобальне інформаційне середовище [3].

У роботі [4] на основі аналізу дефініцій, результати якого наведені в [5], запропоновано поняття кіберпростору, який визначається як віртуальне комунікаційне середовище, утворене системою зв’язків між користувачами та об’єктами інформаційної інфраструктури. У цій же роботі запропоновано поняття інформаційного простору, як глобального інформаційного середовища, яке в реальному часі забезпечує обробку інформації про протиборчі сторони та їх оточення з метою формування оптимальних рішень. Суб’єкт інформаційного простору у процесі своєї діяльності створює інформацію, привласнює її, накопичує і передає. Таким суб'єктом може бути людина, різні соціальні групи, а також компанії, органи державного управління, держава в цілому – всі, хто в ході здійснення господарчої діяльності використовує можливості сучасних інформаційних технологій, але в будь-якому разі інформаційний простір не може існувати без діяльності людини.

Новою сферою інформаційних відносин стала боротьба за розподіл інформаційного простору. До створення глобальної інформаційної мережі поняття «інформаційна боротьба» означало виключно ведення пропаганди через засоби масової інформації (ЗМІ). Ситуація змінилася з появою Інтернету (Interconnected Networks) – глобальної телекомунікаційної мережі інформаційних і обчислювальних ресурсів. У 1991 р. з'явилася основна послуга мережі – Всесвітня павутина (World

Wide Web). Вона спростила пошук інформації і дозволила обслуговувати графічні, відео та аудіофайли. В 1993 р. провідні світові ЗМІ почали використовувати електронну мережу для розміщення електронних версій своїх видань, що дозволило суттєво розширити аудиторію, на яку спрямовувалась та чи інша інформація, а також суттєво зменшити час представлення такої інформації. Цей феномен зробив можливим технічно розв'язати проблему управління інформаційним простором: управління доменними іменами, адресами, інтернет-протоколами, системою кореневих серверів, контентом тощо.

У сучасному світі інформаційний простір, у зв'язку з розвитком сучасних комунікацій, став практично безмежним, що є одним із позитивів, і в той же час така властивість сучасного інформаційного простору провокує процеси порушення комплексної інформаційної безпеки. Проте все ж інформаційний простір має свої рамки, обумовлені офіційними обмеженнями. Ці обмеження бувають конвенціональними – зобов'язуючими дотримуватися комерційної таємниці, що забезпечують право людини на недоторканність приватного життя, та інституційними, пов'язаними, наприклад, з державною або військовою таємницею.

Структура інформаційного простору обумовлена наявністю зв'язків між суб'єктами та об'єктами на які ці суб'єкти мають вплив. Суб'єкти та об'єкти з часом змінюються, переходять з одного стану в інший, утворюючи нові зв'язки і руйнуючи старі, що обумовлює динаміку інформаційного простору. Такі зміни можуть відбуватися через проведення СІО, які з урахуванням наявності людини як об’єкта захисту доцільно розділити на інформаційно-кібернетичні операції (ІКО), що спрямовані на технічну складову СТС, та інформаційно-психологічні операції (ІПО), метою яких є вплив на соціальну складова СТС. Основна проблема полягає в тому, що в інформаційному просторі структури фрагментарні, а зв'язки локальні, тому суб'єкт інформаційного простору іноді може навіть не підозрювати про існування іншого суб'єкта, інформаційно віддаленого від нього. Процеси циркуляція інформації з обмеженим доступом (ІзОД), а також інформації, яка створюється спеціально з метою реалізації деструктивного інформаційного впливу, породжують проблеми, пов’язані із забезпеченням комплексної інформаційної безпеки.

1.2 Методологічні основи проведення кібернетичних атак

Сучасна концепція соціотехнічних систем на противагу теорії технологічного детермінізму, яка стверджує односторонню дію технічної складової системи на людину, ґрунтується на ідеї взаємодії людини і техніки, тобто на взаємозалежних впливах. Соціотехнічна система складається з таких підсистем: технічна підсистема, до якої належать обладнання і технології, що перетворюють певним способом вхідні дані у вихідні, який покращує ефективність функціонування системи; соціальна підсистема, яку утворюють люди, їх знання, уміння, настрій, ціннісні установки та ставлення до виконуваних функцій, управлінська структура і система заохочень. Склад СТС представлений на рис. 1.1.

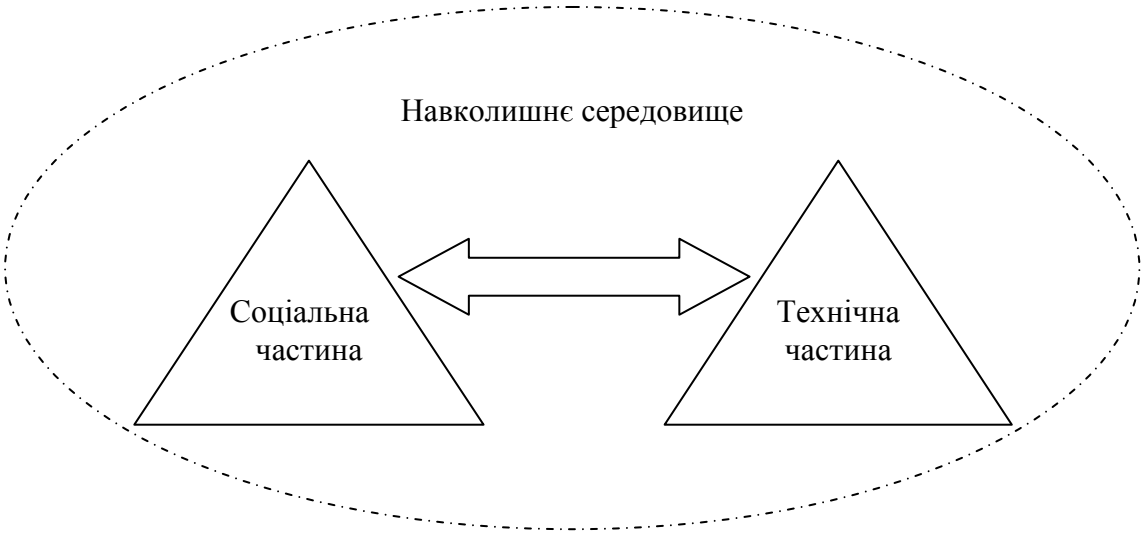

Рисунок 1.1 – Склад соціотехнічної системи

Основними показниками СТС є ефективність, керованість, стійкість, надійність. Беручи до уваги те, що процес життєдіяльності СТС відбувається у певній множині середовищ – навколишньому, виробничому, технологічному, інформаційному тощо, то необхідно враховувати, як важливий чинник, інформаційну взаємодію з іншими системами, що можуть виступати як конкуренти. Беручи до уваги другий закон Джилба «Будь-яка система, яка залежить від надійності людини – ненадійна» та інтерпретуючи його на поняття «інформаційна безпека» і беручи до уваги, що більшість сучасних СТС функціонують у

конкурентному інформаційному середовищі, можна зробити висновок, що забезпечення достатнього рівня комплексної інформаційної безпеки СТС є комплексною актуальною задачею.

Безпека сучасних соціотехнічних систем має декілька складових. Найбільш важливими з них є такі: економічна, екологічна, промислова, інформаційна тощо. На перший погляд незалежні складові комплексної безпеки соціотехнічних систем при більш детальному аналізі представляються вже взаємозалежними. Нескладно представити ланцюжок виникнення ймовірних подій: порушення інформаційної безпеки призводить до порушення екологічної, промислової безпеки, наприклад, якщо розглядати такі об’єкти, як хімічно-небезпечні або атомні станції. Другий приклад. Порушення інформаційної безпеки може призвести до порушення економічної безпеки, якщо розглядати такий об’єкт як певну фінансову установу. Зрозуміло, що таких прикладів можна навести багато.

У роботі [6] висвітлено характерні ознаки та проблемні аспекти кібернетичної безпеки держави, а у роботі [7] зазначено, що розробка і впровадження систем для оцінювання та захисту інформації є обов’язковою умовою розвитку та існування держави. Рішення цієї глобальної проблеми починається з розв’язання задачі забезпечення інформаційної безпеки складних систем, до яких відносяться і різноманітні СТС, зокрема, різноманітні промислові об’єкти та підприємства. Оцінювання рівня інформаційної безпеки представляє собою комплексну задачу, і її рішення вимагає відповідної науково-методичної бази. Ця база повинна визначати механізми створення і реалізації системи захисту, критеріальні оцінки захищеності, а також розв’язувати задачі прогнозування можливих небезпек та методів і засобів боротьби з ними. Розв’зання цієї задачі, як правило, розбивається на такі окремі складові:

– організаційний захист;

– захист програмного забезпечення (баз даних, операційних систем і т. д.);

– захист технічного обладнання;

– нормативно-правовий захист;

– захист від методів соціальної інженерії.

Крім комплексності використання методів інформаційного захисту слід також враховувати пряму або опосередковану соціальну залежність кожного напряму захисту.

З огляду на сказане вище, взаємозалежність ризиків порушення інформаційної безпеки та інших типів безпеки СТС можна представити у вигляді структури, яка зображена на рис. 1.2.

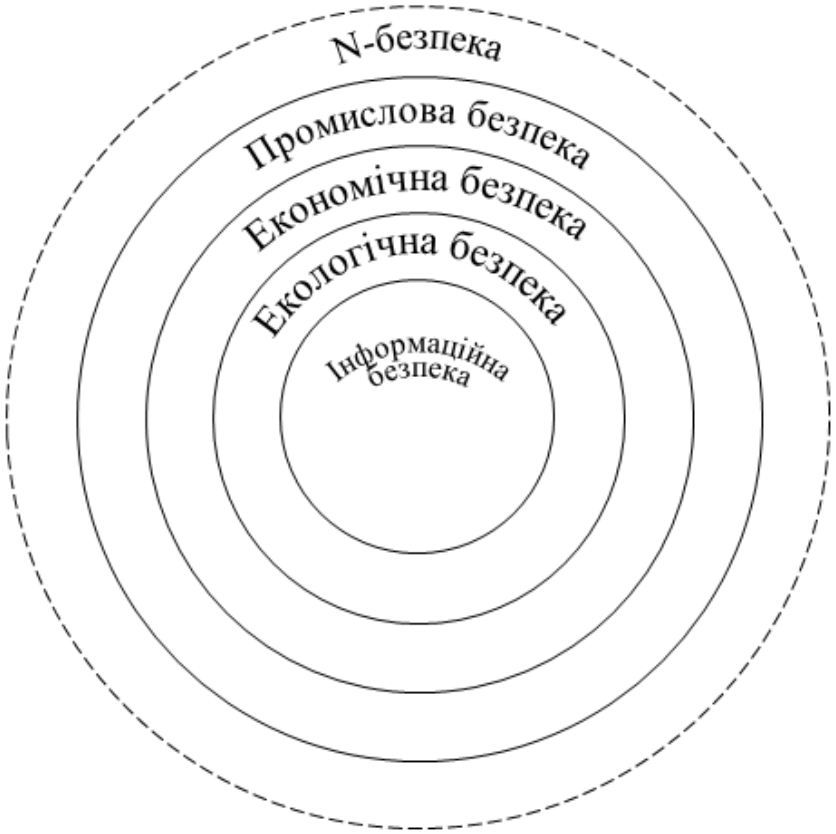

Рисунок 1.2 – Взаємозалежність ризиків порушення інформаційної безпеки

Ядро цієї структури складає інформаційна безпека. Це дозволяє стверджувати, що підвищення рівня інформаційної безпеки ядра зменшує виникнення ризиків економічного, екологічного, промислового походження тощо.

Людина, як активний елемент такої системи може впливати різним чином на розвиток такої системи і, як наслідок, впливати на стан і розвиток множини середовищ, що її оточують. Згідно зі статистикою, наведеною Computer Security Institute (США), основні порушення захисту комп'ютерних систем, які відносяться до СТС, визначаються такими причинами і даними:

– несанкціонований доступ –2 %;
– вірусна загроза – 3 %;
– технічні відмови – 20 %;
– цілеспрямовані дії персоналу – 20 %;
– помилки персоналу – 55 %.

Таким чином, спираючись на наведену статистику, можна зробити висновок, що більша частина порушень пов'язана з людиною. Однак, у цій статистиці не наведено дані, які можна ідентифікувати, як дії людини, що потрапила під дію ІПО. Це означає, що загальний стан інформаційної безпеки СТС доцільно аналізувати через призму інформаційної війни, ефективне проведення якої може суттєво змінити початковий або стійкий стан СТС.

Якщо функціонування СТС представити як взаємодію різнорідних підсистем – соціальної і технічної, то доцільно розглядати взаємний вплив підсистем з урахуванням множини навколишніх середовищ [8].

Стан СТС значною мірою визначає особливості процесу проведення проти неї ІПО і характеризується набором значень відповідних параметрів, наприклад, ймовірнісними оцінками порушень цілісності, конфіденційності та доступності інформаційних ресурсів системи як об'єкта захисту. Це дозволяє розглянути стан системи, як множину точок n-вимірного простору, який характеризується значеннями досліджуваних параметрів [9].

Наприклад, якщо розглядати проведення ІПО на колектив (окрему особу), який працює з відповідним технологічним обладнанням, то процес деструктивного впливу з наступними ймовірними причинно-наслідковими діями передбачає використання множини мемів M_1, які безпосередньо мають вплив на множину виконавців M_2, а ті, у свою чергу, будуть впливати на множину обладнання M_3, та множину інших ресурсів M_4. деструктивний вплив, реалізований, наприклад, за допомогою мема.

У роботі [10] функціонування різнорідних частин СТС пропонується представити як взаємодію детермінованого автомата (ДА), який формалізує технічну частину СТС та недетермінованого автомата (НДА), який представляє соціальну складову.

Схема причинно-наслідкового комплекс, який представляє взаємодію двох різнорідних частин наведена на рис. 1.3.

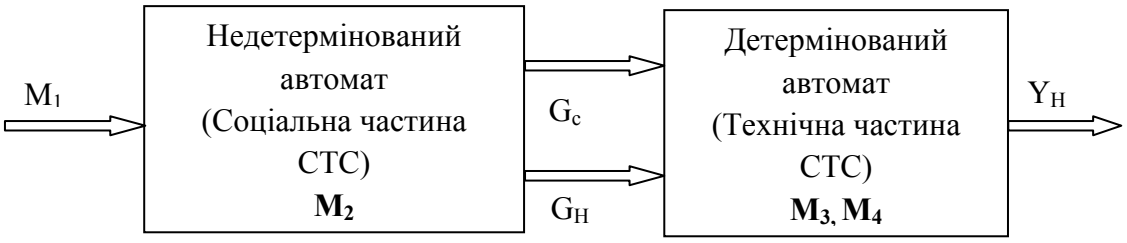

Рисунок 1.3 – Схема причинно-наслідкового комплексу взаємодії частин СТС

Недетермінований автомат може бути представлений як абстрактна система

$$N = (S, Q, G, f, \mu), \tag{1.1}$$

де S – множина вхідних сигналів; Q – множина внутрішніх станів; G, – множина вихідних станів; f – функція переходів; μ – функція виходів.

Стан НДА (соціальної частини СТС) формує вхідний сигнал для ДА або технічної складової СТС, яка може бути описана як система

$$A = (Z, X, Y, \delta, \lambda), \tag{1.2}$$

де Z – множина станів; X, Y – множини вхідних та вихідних сигналів; δ – функція переходів; λ – функція виходів.

На запропонованій схемі на вхід НДА надходить множина $M_1 < S$ яка впливає на соціальну частину СТС множину M_2. Під дією M_1 НДА може перейти у так званий нестійкий стан Q_{H}, або залишитись у стійкому стані Q_{C}. Нестійкий внутрішній стан Q_{H} формує несприятливий вихідний сигнал G_{H} для технічної частини СТС. Такий стан спричинить деструктивний вплив соціальної частини СТС на техніко-технологічну частину СТС або інші ресурси об’єкта захисту, що, у свою чергу, при незадовільному комплексному захисті призведе до нестійкого стану всієї системи, але бажаному стану для суб’єкта, який проводив ІПО, з метою виведення з ладу всієї системи.

Формально, послідовність взаємодії складових СТС типу «причина–наслідок», яка може призвести до виведення всієї системи з ладу може бути представлена такою абстрактно системою відношень:

1. Робота НДА може бути представлена співвідношенням

$$G(t) = f\big(S(t), Q(t)\big), \tag{1.3}$$

2. З урахуванням особливостей проведення ІПО та складу СТС, робота НДА може бути представлена

$$G_{\text{Н}} = f_{\text{Н}}(Q_{\text{Н}}(t), M_1 < S), \tag{1.4}$$

де $G_{\text{Н}}$ – сигнал, який формується нестійким станом НДА.

3. Робота ДА, з урахуванням надходження на його вхід сигналу G_H, може призвести до деструктивного впливу на технічну складову системи, що описується співвідношенням:

$$Y_{\text{Н}}(t) = \delta(G_{\text{Н}} < X, Y_{\text{Н}} < Y). \tag{1.5}$$

Сучасні соціотехнічні СТС функціонують в умовах критичних глобальних змін, основними ознаками яких є:

– різного роду аварії і катастрофи;
– збільшення використання енергії різного походження;
– погіршення стану екології навколишнього середовища;
– терористичні акти.

При цьому життєдіяльність СТС характеризується невизначеністю, яка може бути викликана невчасно отриманою, неповною або навмисно перекрученою інформацією. Варто також відзначити можливість використання конфіденційної інформації потенційними конкурентами у власних цілях, що вже є ознакою інформаційного протиборства.

В останні часи інформаційне протиборство характеризується елементами інформаційної війни, тобто сукупністю спеціальних операцій, спрямованих на певний об’єкт з метою зміни його стану за рахунок зміни його структури або зміни зв’язків між елементами даної структури. Дії, що спрямовуються на об’єкт впливу (ОВ), реалізуються через певні категорії представників суспільства або з використанням засобів масової інформації завдяки штучній зміні їх свідомості та їх особистісного відношення до об’єкта [11, 12]. Суб’єкт, який реалізує спеціальні операції назвемо центром впливу (ЦВ). Таким чином, реалізація технологій інформаційної війни, тобто проведення спеціальних операцій, може бути реалізована за допомогою структури, яка представлена на рис. 1.4.

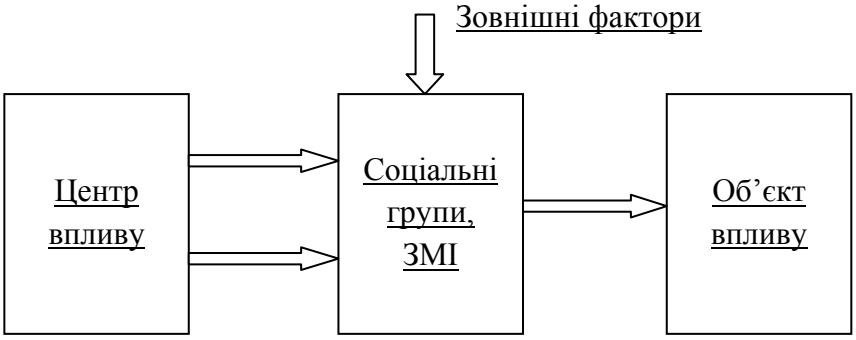

Рисунок 1.4 – Схема реалізації технологій інформаційної війни

Причинами виникнення інформаційних конфліктів може бути проведення виборної компанії, боротьба політичних і економічних еліт за сфери впливу, перерозподіл сфер впливу між корупційними і кримінальними групами, підготовка і проведення терористичних актів, міждержавні конфлікти тощо [13].

Загальними передумовами, що можуть спричинити виникнення інформаційної війни, є:

– розвиток інформаційних технологій, що впливають на свідомість і підсвідомість;

– практична відсутність інформаційних кордонів;

– зростаюча роль керівних кадрів або окремих осіб-спеціалістів на яких може бути спрямована дія інформаційного впливу.

Практична реалізація спеціальних операцій та захист від них реалізується спеціальними структурами – службою захисту інформації (СЗІ) об'єктів взаємодії – СЗІ ЦВ та СЗІ ОВ, функції і задачі якої регламентуються НДТЗІ 1.4-001-2000.

Діяльність СЗІ, яка може бути підрозділом служби безпеки, спрямована на виконання таких інформаційно-аналітичних функцій, виконання яких сприятиме мінімізації можливих втрат [14]:

– забезпечення захисту власних інформаційних ресурсів;

– забезпечення своєчасного отримання надійної інформації з певних питань;

– забезпечення ефективності та уникнення дублювання при збиранні, аналізі і розповсюдженні інформації;

– моделювання сценаріїв поведінки конкурентів, які можуть стосуватись інтересів підприємства;

– здійснення постійного моніторингу конкурентного середовища.

Ефективність отримання інформації щодо конкурентів досягається шляхом комплексного використання різних засобів і заходів, які забезпечують підвищення достовірності інформації. Технологія отримання інформації передбачає такі етапи:

– організація отримання інформації;

– отримання даних і відомостей;

– проведення інформаційно-аналітичної роботи.

Перераховані етапи отримання інформації мають бути інтегровані в єдиний комплекс і, зрозуміло, що всі вони мають велике значення для отримання ефективного результату діяльності СЗІ об’єкта захисту. Однак, останній етап є найбільш значущим, оскільки результатом проведення інформаційно-аналітичної роботи є звіт, який впливає на прийняття управлінського рішення щодо оцінювання та забезпечення інформаційної безпеки об’єкта. Цей звіт забезпечує керівництво підприємства та його різні підрозділи узагальненою інформацією, яка дозволяє комплексно керувати ризиками різних типів. У практичній площині це дозволяє вирішити такі задачі:

– проведення інформаційної експрес-оцінки ймовірних конкурентів, та їх можливих дій;

– інформаційний супровід власних активних дій;

– комплексний контроль стану захищеності власних об’єктів, ресурсів, комунікацій, конфіденційної інформації;

– забезпечення координації і взаємодії функціональних підрозділів підприємства на основі взаємного обміну інформацією.

Розв’язання цих задач дозволяє виявити серед всього оточення ті об’єкти, що мають ознаки зв’язку з ймовірними джерелами загроз – конкурентами, а також ідентифікувати внутрішні загрози, які пов’язані, в першу чергу, з діяльністю людини. Важливою складовою звіту СЗІ об’єкта є прогноз поведінки конкурентів і динаміки змін внутрішніх загроз. Це дозволяє з певною достовірністю оцінити можливі сценарії поведінки конкурентів і визначити механізми ведення спеціальних інформаційних операцій. В більшості випадків застосо-

вуються типові схеми дестабілізації об’єкта, які формалізуються у вигляді впливу на людину, дискредитації керівництва об’єкта, інформаційно-психологічного впливу на громадськість відносно об’єкта впливу, а також систематичне розповсюдження спеціально підібраної інформації.

Зрозуміло, що важливою задачею є створення так званого «дружнього інтерфейсу», через який ЦВ зможе реалізовувати свої задачі. При цьому необхідно враховувати, що ОВ також може знаходитись у двох можливих станах: пасивному та активному. Пасивний стан об’єкта характеризується тим, що він підпадає під повну інформаційну залежність центру впливу, обумовлену тим, що ЦВ має значну перевагу в різних ресурсах: фінансових, інформаційних, ідеологічних тощо. Активний стан об’єкта характеризується тим, що об’єкт проводить відповідні атакуючі або контратакуючі дії.

Розглянемо можливі шляхи реалізації ЦВ своїх задач. Це можуть бути механізми пропаганди, агітації та інформаційного протиборства [15]. Для пасивного стану об’єкта найбільш ефективними є шляхи агітації і пропаганди, оскільки вони спрямовані на зміну свідомості працівників та розповсюдження відповідної інформації, що дозволить змінити стан об’єкта. Інформаційне протиборство передбачає взаємодію конкуруючих структур у боротьбі за лідерство. Зацікавлені люди, як показує практичний досвід, можуть виконувати функції подвійних агентів і реалізовувати як задачі ОВ, так і ЦВ.

На рис. 1.5 представлена структурна модель реалізації механізмів інформаційного впливу, таких як агітація і пропаганда [16].

Модель враховує створення «дружнього інтерфейсу впливу», через який підготовлена інформація певним чином впливає на потенційного конкурента. Керівництво об’єкта впливу, враховує підготовлену інформацію, яка є для нього вхідною і приймає відвідні управлінські рішення щодо забезпечення необхідного рівня інформаційної безпеки.

Структурна модель реалізації інформаційного протиборства представлена на рис. 1.6 і формалізує процеси взаємодії двох конкуруючих суб’єктів, що можуть спричинити зміни інформаційних зв’язків між їх елементами і, як наслідок, зміну їх структури і перехід об’єкта в інший стан [16].

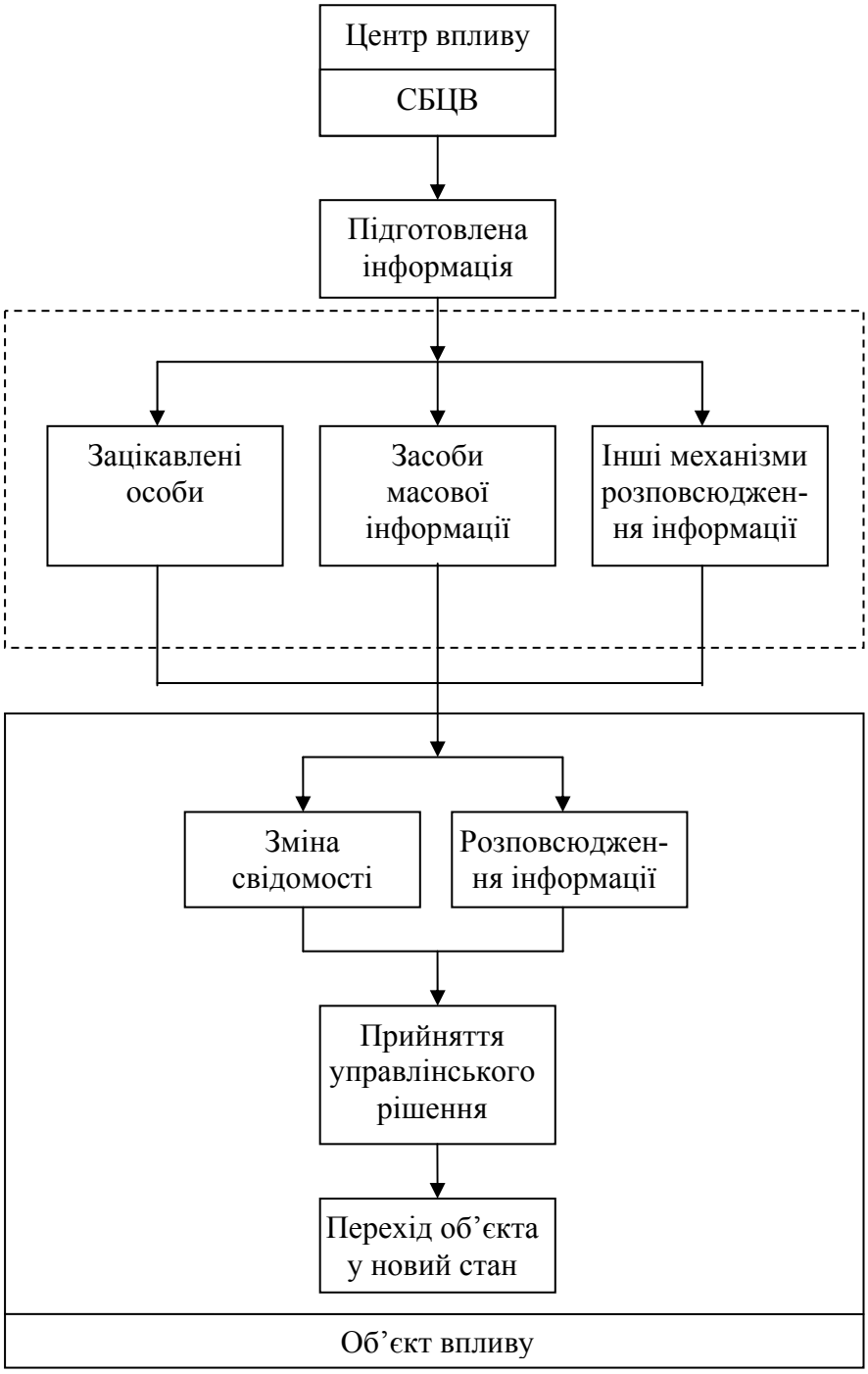

Рисунок 1.5 – Структурна модель механізмів агітації і пропаганди

Зміна зв’язків між елементами об’єкта або перехід його у інший стан може супроводжуватись зниженням рівня інформаційної безпеки. Інформаційний вплив починається з певної послідовності дій з боку конкурента. Такі дії для будь-якого зовнішнього спостерігача представляються спеціально підготовленою інформацією, що знаходить відображення в новинах, які отримуються як з відкритих джерел ін-

формації, так і здобуваються за допомогою спеціальних технічних засобів і технологій, а також агентурним шляхом.

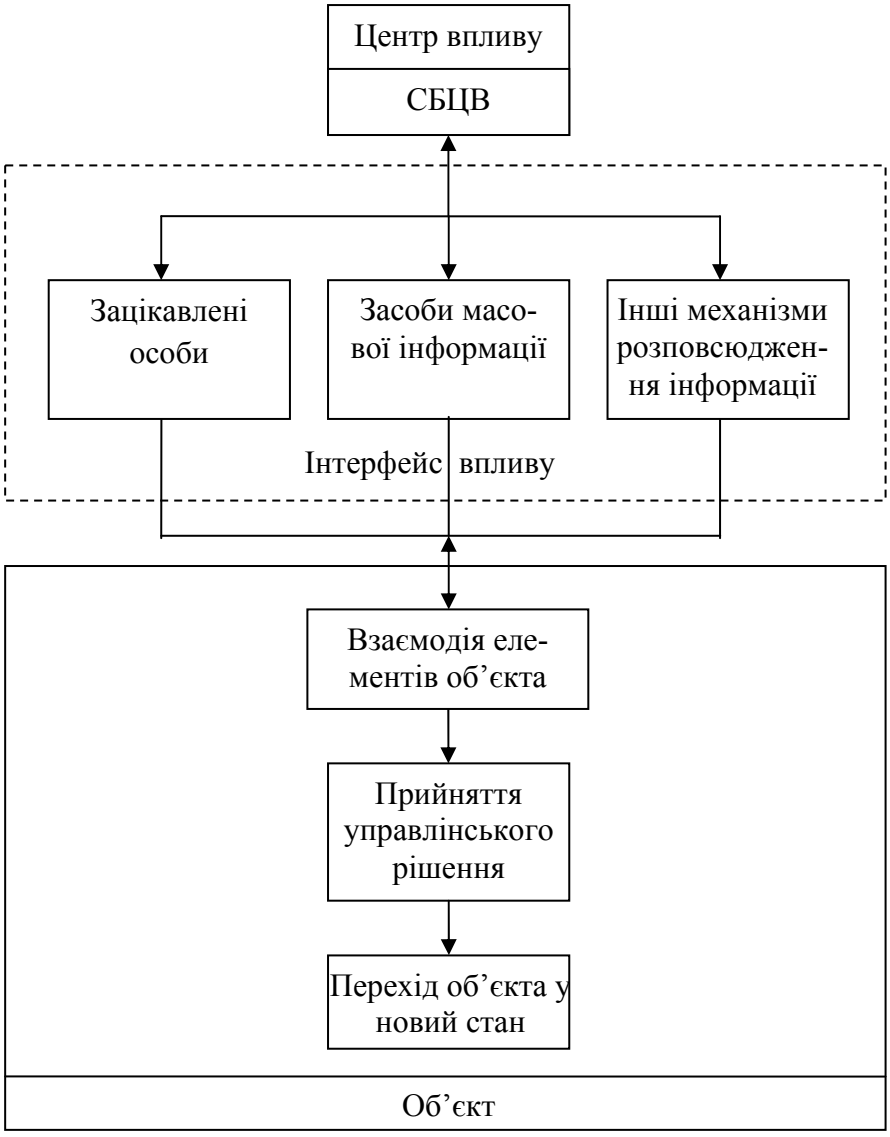

Рисунок 1.6 – Структурна модель механізму інформаційного протиборства

Тому для соціотехнічних систем, до яких належать і сучасні підприємства, що функціонують у множині конкурентних середовищ, важливим є організація у структурі СЗІ інформаційно-аналітичної служби, основними задачами якої є мінімізація результатів інформаційного впливу з боку конкурентів, а також планування і проведення власних СІО з метою покращення стану об'єкта захисту.

При проведенні спеціальної СІО, зокрема ІПО, яка є механізмом проведення агітації, пропаганди і інформаційного протиборства і

ПЕРЕЛІК ПОСИЛАНЬ

1. Thomas P. Rona, “Weapon Systems and Information War”, Boeing Aerospace Co.,Seattle, WA, 1976. – Режим доступу до ресурсу: http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf

2. Президент ввів у дію рішення РНБО про Головний ситуаційний центр [Електронний ресурс] – Режим доступу до ресурсу: http://www.ukrinform.ua/rubric-iac/1820573-porohenko_vviv_u_diyu [Назва з екрану].

3. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки : монографія/ В. Л. Бурячок. – К. : НАУ, 2013.— 432 с.

4. Інформаційна та кібербезпека: соціотехнічний аспект / В. Л. Бурячок, В. Б. Толубко, С. В. Хорошко, С. В. Толюпа. – К. : ДУТ, 2015. – 288 с.

5. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк // Безпека інформації . – 2015. – Т. 19, № 2. – С. 118–129.

6. Корченко О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О. Г. Корченко, В. Л. Бурячок, С. О. Гнатюк // Безпека інформації. – 2013. – Т. 19, № 1. – С. 40–45.

7. Лужецький В. А. Оцінка інформаційної безпеки підприємства. / В. А. Лужецький, А. В. Дудатьєв, Ю. В. Баришев // Вісник Черкаського технологічного університету. – №1. – 2005. – С. 50–53.

8. Харченко В. С. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения / В. С. Харченко.– Харьков : Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», 2011. – 641 с.

9. Дудатьев А. В. Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны / А. В. Дудатьєв, В. А Лужецкий, Д. А. Коротаев // Восточно-Европейский журнал передовых технологий. – 2016. – № 1. – С. 4–11.

10. Лужецький В. А. Взаємодія типу «причина–наслідок» складових соціотехнічних систем / А. В. Лужецький, А. В. Дудатьєв // Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS’2017) : науково-практична конференція, 20–23 червня 2017 р. : тези доповідей. – Миколаїв : С. 53–55.

11. Хорошко В. О. Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. Ч. 1. / В. О. Хорошко, Ю. Є Хохлачова // Безпека інформації. – 2016. – Т. 22, № 3 – С. 283–288.

12. Polishchuk Yu. Mass media as a channel of manipulative influence on society / Yu. Polishchuk, S. Gnatyuk, N. Seilova // Ukrainian Scientific Journal of Information Security. – 2015. – V. 21, № 3. – P. 301–308.

13. Пєвцов Г. В. Модель регіону України як об'єкта забезпечення інформаційної безпеки / Г. В. Пєвцов // Системи обробки інформації. – 2010. – № 5 (86). – С. 2–9.

14. Лужецький В. А. Інформаційна безпека / В. А. Лужецький, О. П. Войтович, А. В. Дудатьєв. – Вінниця : Універсум-Вінниця, 2009. – 239 с.

15. Цыганов В. В. Интеллектуальные механизмы информационных войн / В. В. Цыганов, С. Н. Бухарин, В. В. Васин // Проблемы управления. – 2007. – № 1. – С. 25–30.

16. Дудатьєв А. В. Інформаційна безпека соціотехнічних систем в умовах інформаційної війни / А. В. Дудатьєв // Інформаційні технології та комп'ютерна інженерія. – 2011. – № 3(22). – С. 75–79.

17. Вовк В. М. Основи системного аналізу // В. М. Вовк, З. Б. Дрогомирецька. – Львів : ЛНУ ім. Івана Франка, 2002. – 248 с.

18. Дудатьєв А. В. Аксіоматика теорії комплексної безпеки соціотехнічних систем / А. В. Дудатьєв // Інформаційні технології та комп'ютерна інженерія. – 2013. – № 1(26). – С. 22–25

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

20. Дудатьєв А. В. Методологічні основи інформаційних війн / А. В. Дудатьєв // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації : науково-практична конференція, 25–28 лютого 2015 р. тези доповідей. – Київ : Європейський університет, 2015. – С. 37–39.

21. Гізун А. І. Аналіз сучасних теорій інформаційно-психологічних впливів в аспекті інформаційного протиборства / А. І. Гізун, В. С. Гріга // Безпека інформації . – 2016. – Т. 22, № 3 – С. 272–282.

22. Бурячок В. Л. Можливість забезпечення захисту від інформаційно-психологічного впливу на основі універсального методу онто-

логій / В. Л. Бурячок, А. А. Шиян // Сучасний захист інформації. – 2013. – № 4. – С.57–67.

23. Грищук Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі / Р. В. Грищук, І. О. Канкін, В. В. Охрімчук // Захист інформації. – 2015. – Т. 17, № 1. – С. 80–86.

24. Van Niekerk B. The Information Warfare Life Cycle Model / B. Van Niekerk, M. S. Maharaj // SA Journal of Information Management – 2011. – V. 13, № 1. – P. 9.

25. Cox L. Planning for psychological operations: a proposal / L. Cox. // Air Command and Staff College, Maxwell Air Force Base. – Montgomery, Alabama, 1997. – 89 p.

26. Pew R.W. Modeling Human and Organizational Behavior: Appliction to Military Simulations / Richard W. Pew, Anne S. Mavor. – Washington, D.C. : National Academy Press, 1998. – 418 p.

27. Jormakka J. Modeling Information Warfare as a Game / Jorma Jormakka, Jarmo V. E. Mölsä // Journal of Information Warfare. – 2005. – V. 4 (2), № 12. – 25 p.

28. Hutchinson B. Information Warfare: Using the Viable System Model as a framework to attack organizations / B. Hutchinson, M. Warren. Режим доступу до ресурсу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.624.63&rep=rep1&type=pdf.

29. Докинз Р. Эгоистический ген / Р. Докинз. – М. : Мир, 1993. – 318 с.

30. Brodie R. Virus of the mind: The new science of the meme. – Hay House, Inc, 2009. Режим доступу до ресурсу: https://docs.google.com/viewerng/viewer?url=http://www.kimhartman.se/wp-content/uploads/2013/09/Virus-of-the-mind-summary.pdf

31. Артёмов А. А. Теоретические основы информационного управления / А. А. Артёмов // Информационные войны. – 2015. – № 3. – С. 83–97.

32. Леоненко С. Рефлексивное управление противником // Армейский сборник. – 1995. – № 8. – С. 27–32.

33. Андрєєва, О. М. Кіберзброя та аналіз її деструктивної діяльності на прикладі впливу вірусу нового покоління STUXNET на іранську ядерну програму / О. М. Андрєєва, К. Мусієнко // Actual problems of international relations. – 2014. – Т. 1, № 103.

34. Sharp Gene 198 Methods of non violent action from Tne Politics of Nonviolent Action / G. Sharp//Bos, Porter Sargent,1973. – Режим доступу до ресурсу: http://www.youthpolicy.org/library/documents/198-methods-of-nonviolent-action/

35. Дедков В. К. «Улучшение состояния системы» как форма скрытой атаки посредством запуска «критических технологий» / В. К. Дедков, В. П. Баранов // Надежность и качество : международный симпозиум : труды международного симпозиума. – Пенза, 2011. – Т. 2. – С. 26–28.

36. Дудатьєв А. В. Технологии информационной войны: мемпрограммирование / А. В. Дудатьєв // Безпека інформації. – 2016. – Т. 23, № 1. – С. 41–46.

37. Лужецький В. А. Концептуальна модель системи інформаційного впливу / В. А. Лужецький, А. В. Дудатьєв // Безпека інформації. – 2017. – Том 23, № 1. – С. 45–49.

38. Михайлов А. П. Модели информационной борьбы [Електронний ресурс] / А. П. Михайлов, Н. А. Маревцева // Математическое моделирование. – 2011. – Т. 23, № 10. – С. 19–32. – Режим доступу: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=mm&paperid=3162&option_lang=rus.

39. Михайлов А. П. О свойствах простейшей математической модели распространения информационной угрозы / А. П. Михайлов, Н. В. Клюсов // Математическое моделирование социальных процессов. – М. : МАКС Пресс, 2002. – Вып. 4. – С. 115–123.

40. Маревцева Н. А. Простейшие математические модели информационного противоборства / Н. А. Маревцева // Математическое моделирование социальных процессов. – М. : МАКС Пресс, 2010. – Вып. 11. – С. 59–72.

41. Маревцева Н.А. Некоторые математические модели информационного нападения и информационного противоборства / Н. А. Маревцева // Социология. – 2011. – № 3. – С. 26–35.

42. Михайлов А. П. Об оптимальном управлении процессом распространения информации / А. П. Михайлов, К. В. Измоденова // Математическое моделирование. – 2005. – Т. 17, № 5. – С. 67–76.

43. Михайлов А. П. Об оптимальном управлении в математической модели распространения информации / А. П. Михайлов, К. В. Измоденова // Труды семинара «Математическое моделирование социальных процессов» : сборник. – М. : МАКС Пресс, 2004. – Вып. 6.

44. Маревцева Н. А. Простейшие математические модели информационного противоборства / Н. А. Маревцева // Математическое моделирование и современные информационные технологии : сборник трудов Всероссийских научных молодежных школ. – Ростов-на-Дону : Южный федеральный университет, 2009. – Выпуск 8. – С. 354–363.

45. Михайлов А. П. Модели информационной борьбы / А. П. Михайлов, Н. А. Маревцева // Математическое моделирование. – 2011. – Т. 23, № 10. – С. 19–32.

46. Bass F.M. A new product growth for model consumer durables / F. M. Bass // Management Science. – 1969. – V. 15. – P. 215–227.

47. Делицын Л. Л. Количественные модели распространения нововведений в сфере информационных и телекоммуникационных технологий / Л. Л. Делицын. – М. : МГУКИ, 2009. – 106 с.

48. Шведовский В. А. Моделирование распространения информации в смежных социальных группах / В. А. Шведовский // Математические методы в социологическом исследовании. – М. : Наука, 1981. – С. 207–214.

49. Chenhao Tan. Adamic Lostin Propagation? Unfolding News Cycles from the Source [Електронний ресурс] / Chenhao Tan // Proceedings of the Tenth International Conference on Web and Social Media (ICWSM 2016) – С. 378–387. – Режим доступу http://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13011.

50. Gnatyuk S. Information-Psychological Security of Society in the Context of Information Warfare / Gnatyuk S., Zhmurko T. // Inżynier XXI wieku projectujemy przyszlosc, monografia / pod red Jacek Rysiński. – Bielsko-Biała : Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016. – С. 321–341.

51. Губанов Д. А. Социальные сети: модели информационного влияния, управления и противоборства /Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили. – М. : Физматлит, 2010. – 225 с.

52. Дудатьєв А. В. Інформаційна безпека соціотехнічних систем: модель інформаційного впливу / А. В. Дудатьєв, О. П. Войтович // Інформаційні технології та комп'ютерна інженерія. – 2017. – № 1(22). – С. 75–79.

53. Бурячок В. Л. До питання організації та проведення розвідки у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко // Наука і оборона. – 2011. – № 2. – С. 19–23.

54. Бурячок В. Л. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем / В. Л. Бурячок, О. Г. Корченко // Захист інформації. – 2012. – № 4(57). – С. 5–12.

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

56. Bespalova B.P. The role of the mass media in changing public opinion. Using the mass media as an ideological weapon / B. P. Bespalova, A. V. Fedorov // The Russian Academic journal. – 2014. – V. 23, № 1. – P. 40–42.

57. Дудатьєв А. В. Моделі для організації протидії інформаційним атакам / А. В. Дудатьєв // Захист інформації. – 2015. – № 2. – С. 157–162.

58. Дудатьєв А. В. Інформаційна обфускація: методи і моделі / А. В. Дудатьєв // Сучасний захист інформації. – 2015. – № 4. – С. 56–61.

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

60. Расторгуев В. П. Информационные операции в сети Интернет / В. П. Расторгуев, М. В. Литвиненко. – М. :АНО ЦСоиП, 2014. – 128 с.

61. 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.

62. Архипов О. Е. Застосування методології передбачення для оцінювання шкоди заподіяної витоком секретної інформації / О. Е. Архипов, І. Касперський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – № 2(15). – С. 13–18.

63. Количество интернет-пользователей в Украине.[Electronic resource]. – 2013. – Available at: http://podrobnosni.ua922673-kolichestvonternetpolzovatelej-v-ukraine.

64. Колесник І. С. Оцінка впливу витоку інформації на стан підприємства / І.С. Колесник, А. В. Дудатьєв, О. П. Войтович // Системи обробки інформації. – 2010. – № 5. – С. 224–229

65. Боровська Т. М. Основи теорії управління та дослідження операцій : навчальний посібник / Т. М. Боровська, І. С. Колесник, В. А. Северілов. – Вінниця : УНІВЕРСУМ-Вінниця, 2008. – 242 с.

66. Боровська Т. М. Оптимізація розподілу обмеженого ресурсу у виробничій системі на базі агрегування виробничих функцій /

Т. М. Боровська, І. С. Колесник, В. А. Северілов // Інформаційні технології та комп'ютерна інженерія. − 2005. – № 1. – С. 12–18.

67. Боровська Т. М. Моделювання розвитку підприємства «на фоні» підприємств і споживачів сегменту ринку / Т. М. Боровська, І. С. Колесник, В. А. Северілов // Вісник ВПІ. – 2009. – № 1. – С. 28–36.

68. Колесник І. С. Розробка імітаційних моделей для оцінки ризиків ринку / І. С. Колесник, П. В. Северілов, В. А. Северілов // Економічна безпека сучасного підприємства : матеріали V Міжн. НПК. – Вінниця : УНІВЕРСУМ-Вінниця, 2008. – С. 66–71.

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

70. Архипов А. Е. Особенности анализа рисков в информационно-коммуникационных системах / А. Е. Архипов // Захист інформації. – 2012. – № 4. – С. 18–27.

71. Дудатьєв А. В. Метод управления комплексной информационной безопасностью / А. В. Дудатьєв // Безпека інформації. – 2015. – Т. 21, № 2. – С. 207–212

72. Корченко А. Г. Анализ и оценивание рисков информационной безопасности / А. Г. Корченко, А. Е. Архипов, С. В. Казмирчук. – К. : Лазурит-Полиграф, 2013. – 275 с.

73. Джордж М. Л. Бережливое производство шесть сигм в сфере услуг / М. Л. Джордж. – М. : Альпина Бизнес Букс, 2005. – 402с.

74. IBM Security Services 2014 Cyber Security Intelligence Index [Electronic resource] – 2014. – Available at: http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

75. Чистяков В. П. Курс теории вероятностей / В. П. Чистяков. – М. : Наука, 1987. – 240 с.

76. Дружинин В. В. Введение в теорию конфликта / В. В. Дружинин, Д. С. Конторов, М. Д. Конторов. – М. : Радио и Связь, 1989. – 288 с.

77. Панарин И. Н. Первая мировая информационная война. Развал СССР / И. Н. Панарин. – СПб. : Питер, 2010. – 256 с.

78. Дудатьєв А. В. Комплексный метод противодействия информационно-психологическим атакам / А. В. Дудатьєв // Проблемы управления и информатики. – 2017. – № 1. – С. 148–155.

79. Dudatyev A. V. Complex Method of Informational-Psychological Operations Counteraction / A. V. Dudatyev // Journal of Automation and Information Sciences. – 2017. – V. 49. – 2017. – P. 76–83.

80. Барлоу Р., Прошан Ф. Математическая теория надежности / Р. Барлоу, Ф. Прошан. – М. : Советское радио, 1969. – 488 с.

81. Дудатьєв А. В. Редактор дерева ризику-відмов / А. В. Дудатьєв, Ю. В. Баришев // Інформаційні технології та комп'ютерна інженерія. – 2007. – № 1(8). – С. 75–79.

82. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / В. Л. Бурячок, О. Г. Корченко, В. О. Хорошко, В. А. Кудінов // Захист інформації. – 2013. – Т. 15, № 1. – С. 5–14.

83. Архипов О. Е. Системний підхід до оцінювання ефективності захисту державної таємниці / О. Е. Архипов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – № 10. – С. 18–22.

84. Вильский, Г. Б. Информационные риски судовождения / Г. Б. Вильский // Науковий вісник ХДМА. – 2012. – № 1(4). – С. 17–26.

85. Лахно В. А. Підвищення кібербезпеки транспорту в умовах деструктивного впливу на інформаційно-комунікаційні системи / В. А. Лахно, А. В. Грабарєв // Восточно-Европейский журнал передовых технологий. – 2016. – № 1. – С. 4–11.

86. Ситуационные центры в решении проблем информационной безопасности [Електронний ресурс] – Режим доступу до ресурсу: http://www.itsec.ru/articles2/Inf_security/sit_cents [Назва з екрану].

87. Дудатьєв А. В. Моделі інформаційної підтримки управління комплексною інформаційною безпекою / А. В. Дудатьєв, О. П. Войтович // Радіоелектроніка, інформатика, управління. – 2017. – № 1. – С. 107–114.

88. Ильин Н. И. Ситуационные центры. Опыт, состояние, тенденции развития / Н. И. Ильин, Н. Н. Демидов, Е. В. Новикова. – М. : МедиаПресс, 2011. – 336 с.

89. 89. Ротштейн А. П. Интеллектуальные технологии идентификации: нечёткие множества, генетические алгоритмы, нейронные сети. / А. П. Ротштейн. – Винница : УНИВЕРСУМ–Винница, 1999. – 320 с.

Наукове видання

Дудатьєв Андрій Веніамінович

КОМПЛЕКСНА ІНФОРМАЦІЙНА БЕЗПЕКА СОЦІОТЕХНІЧНИХ СИСТЕМ: МОДЕЛІ ВПЛИВУ ТА ЗАХИСТУ

Монографія

Редактор С. Малішевська
Оригінал-макет підготовлено автором

Підписано до друку 1.11.2017 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. др. арк. 7,39.
Наклад 300 (1-й запуск 1–75) пр. Зам № В2017-28

Вінницький національний технічний університет,
ІРВЦ ВНТУ,
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ,
ГНК, к. 114.
Тел. (0432) 59-85-32.
publish.vntu.edu.ua; *email*: kivc.vntu@gmail.com.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано ФОП Барановська Т. П.
21021, м. Вінниця, вул. Порика, 7.
Свідоцтво суб'єкта видавничої справи
серія ДК № 4377 від 31.07.2012 р.