УДК 355.01

А.В. ДУДАТЬЄВ

Вінницький національний технічний університет, Вінниця

ІНФОРМАЦІЙНА БЕЗПЕКА СОЦІОТЕХНІЧНИХ СИСТЕМ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Анотація. У статті розглянуто умови функціонування соціотехнічних систем. Запропоновано структурні моделі механізмів ведення інформаційної війни, які дозволяють забезпечити необхідний рівень інформаційної безпеки сучасного підприємства.
Ключові слова: Інформаційна безпека, соціотехнічні системи, інформаційна війна.
Аннотация. В статье рассмотрены условия функционирования социотехнических систем. Предложены структурные модели механизмов ведения информационной войны, которые позволяют обеспечить необходимый уровень информационной безопасности современного предприятия.
Ключевые слова: Информационная безопасность, социотехническая система, информационная война.
Annotation. Operating of the sociotechnical systems conditions are considered in the article. The structural models of mechanisms are offered prosecutions of information war, which allow to provide necessary informative strength of modern enterprise security.
Key words: Safety of information, sociotechnical system, information war.

Вступ

Сучасна концепція соціотехнічних систем (СТС) в протилежність теорії технологічного детермінізму, яка стверджує односторонню дію технології на людину, грунтується на ідеї взаємодії людини і техніки, тобто на взаємозалежних впливах. Соціотехнічна система складається з таких підсистем: технічна підсистема включає пристрої, інструменти і технології, що перетворюють вхідні дані у вихідні певним способом, який покращує ефективність функціонування системи; соціальна підсистема включає людей, їх знання, уміння, настрій, ціннісні установки, відношення до виконуваних функцій, управлінську структуру, систему заохочень. Основними показниками СТС є: ефективність, керованість, стійкість, надійність. Беручи до уваги те, що процес життєдіяльності СТС відбувається у певному середовищі – навколишньому, виробничому, технологічному тощо, то необхідно враховувати важливі чинники – такі як взаємодію з іншими системами – організаціями, 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 «безпека» і розуміючи, що більшість сучасних СТС функціонує у конкурентному середовищі, можна зробити висновок, що забезпечення достатнього рівня комплексної безпеки є важливою задачею.

Актуальність

Безпека сучасних соціотехнічних систем складається з декількох 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 ймовірних ризиків таких 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 ще багато.

Підсумовуючи наведені приклади, взаємозалежність ризиків різних типів можна представити у вигляді структури, яка зображена на рис.1.

Ядро даної структури складає інформаційна безпека.Це дозволяє стверджувати, що підвищення рівня інформаційної безпеки зменшує ризики економічної, екологічної, промислової тощо.

Мета

Метою даної роботи є аналіз механізмів проведення інформаційної війни між двома конкуруючими об’єктами та структурна формалізація механізмів впливу – агітації та пропаганди й інформаційного протиборства.

Постановка задач

1. Виконати аналіз умов функціонування сучасної СТС як критичної системи в умовах інформаційної війни.
2. Розробити структурну модель механізмів агітації і пропаганди.
3. Розробити структурну модель механізму інформаційного протиборства.

Розв’язання задачі

Одним з головних показників стану будь-якої складної системи є її надійність, для сучасної соціотехнічної системи таким показником є її безпека. Людина, як активний елемент такої системи, впливає різним чином на розвиток такої системи і як наслідок впливає на стан і розвиток оточуючого середови-

ща: техногенного, виробничого, екологічного, інформаційного тощо. Сучасні соціотехнічні системи функціонують в умовах критичних глобальних змін, основними ознаками яких є такі:

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

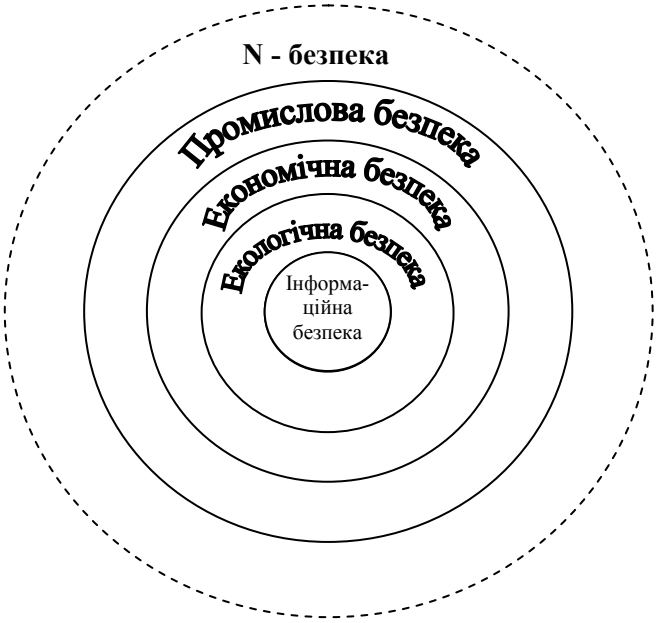

Рисунок 1 – Взаємозалежність ризиків

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

В останні часи інформаційне протиборство типу (захист ↔ напад) характеризується елементами інформаційної війни, тобто сукупністю спеціальних операцій, спрямованих на певний об'єкт з метою зміни його стану або структури. Дії, що спрямовуються на об'єкт впливу (ОВ), реалізуються через певну категорію людей або з використанням засобів масової інформації (ЗМІ) завдяки штучній зміні їх свідомості та їх особистого відношення до об'єкту. Суб'єкт, який реалізує спеціальні операції назвемо центром впливу (ЦВ). Таким чином, реалізація технологій інформаційних війн, тобто проведення спеціальних операцій, може бути реалізована за допомогою структури, яка представлена на рис. 2.

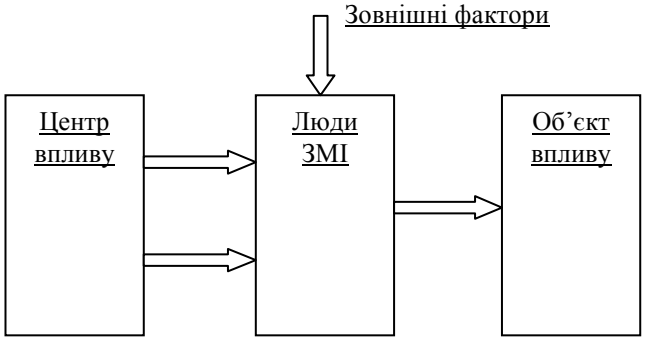

Рисунок 2 – Схема реалізації технологій інформаційної війни

Умовами виникнення інформаційних конфліктів є виборні компанії, боротьба політичних і економічних еліт за сфери впливу, перерозподіл сфер впливу корупційними і кримінальними групами, підготовка і проведення терористичних актів тощо. [1] 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, на яких може бути спрямована дія інформаційного впливу. Практична реалізація спеціальних операцій

впроваджується спеціальними структурами – службами безпеки (СБ) об’єктів взаємодії – СБЦВ та СБОВ.

Діяльність служби безпеки спрямована на виконання таких функцій [2]:

- 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 СБ об’єкта. 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 дозволяю 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. Вирішення цих задач дозволяє виявити серед всіх оточуючих об’єктів таких, які 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 СБ 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 інформаційної війни. В більшості випадків застосовуються 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 об’єкт впливу (ОВ) також може знаходитись у двох можливих станах: пасивному і активному. Пасивний стан об’єкта характеризується тим, що він підпадає під повну інформаційну залежність центру впливу, обумовлену тим, що ЦВ має значну перевагу у 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 [3]. 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’єкту. 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. З урахуванням цього структура інформаційного протиборства представлена на рис.3.

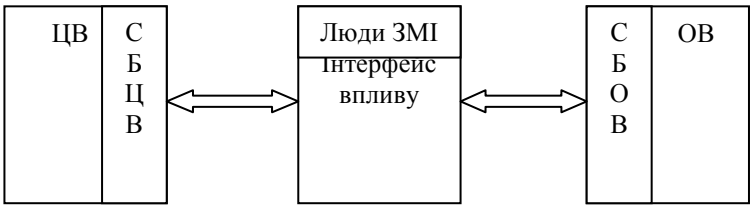

Рисунок 3 – Реалізація інформаційного протиборства

На рис.4 представлена структурна модель реалізації механізмів інформаційного впливу, таких як агітація і пропаганда. Модель враховує створення “дружнього інтерфейсу впливу”, через який підготовлена інформація певним чином впливає на потенційного конкурента. Керівництво об’єкту впливу, вра-

ховує підготовлену інформацію, яка є для нього вхідною і приймає відвідні управлінські рішення, у тому числі щодо забезпечення необхідного рівня інформаційної безпеки.

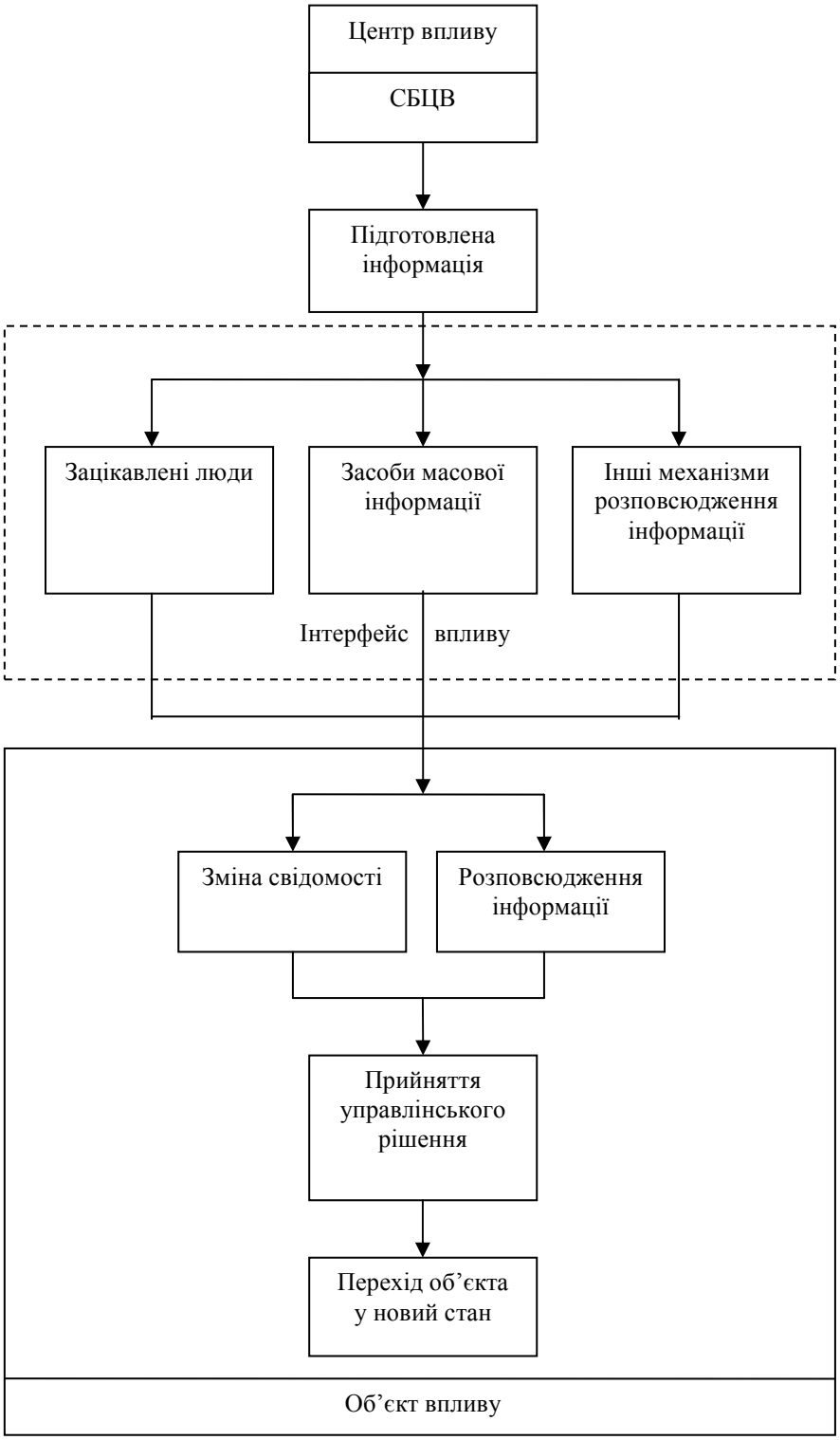

Рисунок 4 – Структурна модель механізмів агітації і пропаганди

Структурна модель реалізації інформаційного протиборства представлена на рис.5 і формалізує процеси взаємодії двох конкуруючих суб'єктів, що можуть призвести до змін інформаційних зв'язків між їх елементами і, як наслідок, зміни їх структури і переходу об'єкта в інший стан. Зміна зв'язків між елементами об'єкта або перехід його у інший стан супроводжується зниженням рівня інформаційної безпеки. Тому для соціотехнічних систем, до яких відносяться і сучасні підприємства, які функціонують

у конкурентному середовищі, важливим є таке правило: “ Необхідно захищати інформацію і захищатись від інформації ”.

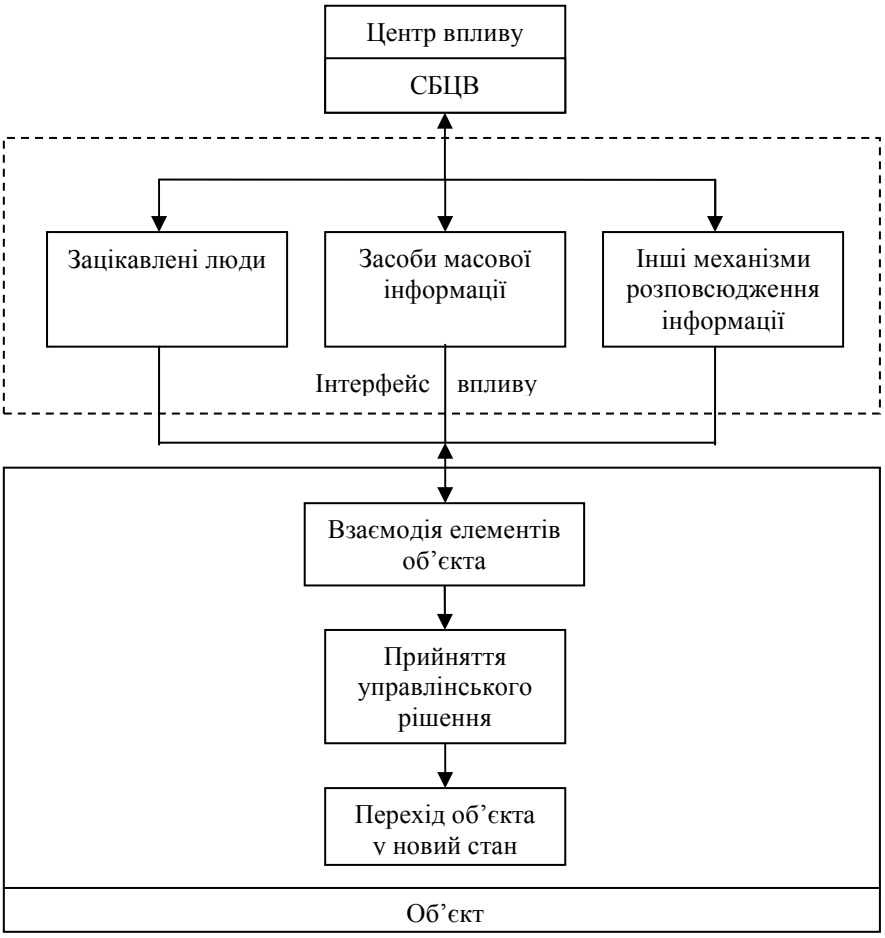

Рисунок 5 – Структурна модель механізму інформаційного протиборства

Висновок

Інформаційні війни є ефективним засобом оволодіння ресурсами. Механізми агітації, пропаганди та інформаційного протиборства забезпечують взаємодію конкуруючих об’єктів із застосуванням елементів інформаційної війни. В статті запропоновані структурні моделі реалізації механізмів ведення інформаційної війни – механізмів агітації і пропаганди та інформаційного протиборства, які можуть використовуватись для досягнення головної мети – забезпечення лідерства на певному сегменті сучасного ринку.

Список літератури

1. Пєвцов Г.В.. Модель регіону України як об’єкту забезпечення інформаційної безпеки / Г.В. Пєвцов // Систми обробки інформації. – Харків.:, 2010. – №5 (86). – С. 2-9.

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

3. Цыганов В.В. Интелектуальные механизмы информационных войн / В.В. Цыганов, С. Н. Бухарин, В.В. Васин // Проблемы управления. – М.:, 2007. – №1. – С. 25-30.

Стаття надійшла: 30.03.2011.

Відомості про авторів

Дудатьєв Андрій Веніамінович – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, вул. Хмельницьке шосе 95, м. Вінниця, Україна (0432) 598485