Концептуальний підхід забезпечення комплексної інформаційної безпеки соціотехнічної системи

Дудатьєв А. В., Літушко О. А.

кафедра захисту інформації
Вінницький національний технічний університет,
Вінниця, Україна
dudatyev.av@gmail.com

Conceptual approach to the comprehensive information security of the sociotechnical system

Andriy Dudatyev, Olena Litushko

Department of information security
Vinnytsia National Technical University
Vinnytsia, Ukraine
dudatyev.av@gmail.com

Анотація **– Технології інформаційної війни принципово змінюють підходи щодо рішення задач оцінювання та забезпечення комплексної інформаційної безпеки. Актуальною проблемою є реалізація захисту соціуму від спеціальних інформаційно-психологічних операцій. 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. Зокрема, запропоновано гнучкий комплексний FC-метод, що дозволяє ефективно розв'язувати задачі з комплексного захисту інформації з урахуванням специфіки етапів проектування та експлуатації КСЗІ в умовах ведення інформаційного протиборства на рівні «підприємство–регіон–держава». Представлено метод інформаційної обфускації, метою якого є заплутування соціальної частини соціотехнічної системи. Запропоновано метод мем-програмування, метою якого є оптимальне проведення інформаційно-психологічної операції. Представлено метод оцінювання інформаційної стійкості соціотехнічної системи, а також комплексний метод протидії інформаційно-психологічним операціям, який використовує випереджувальні та компенсувальні меми. Запропоновано структурну модель багаторівневого інформаційно-аналітичного центру управління комплексною інформаційною безпекою. Результати проведених досліджень показали можливість використання даного підходу для рішення задач оцінювання та управління комплексною інформаційною безпекою багаторівневою соціотехнічною системою.**

Ключові слова: соціотехнічна система, комплексна інформаційна безпека, інформаційна війна, спеціальні інформаційні операції, інформаційно-аналітичний центр, підтримка прийняття рішень.

Abstract - Information warfare technologies fundamentally change approaches to solving problems of evaluation and providing comprehensive information security. An actual problem is the implementation of the protection of society from special information and psychological operations. The axiomics of the theory of information interaction type "object-subject" and the classification of information viruses that can be used to "infect" the social part of the sociotechnical system are proposed. The model of information influence and models and methods of counteraction to special cybernetic operations are presented. In particular, a flexible integrated FC-methodology is proposed, which allows to efficiently solve the problem of complex information protection, taking into account the specific stages of the design and operation of KSCI in the context of conducting an information confrontation at the enterprise-region-state level. The method of information obfuscation is presented, the aim of which is to obscure the social part of the sociotechnical system. A method of mem-programming is proposed, the purpose of which is to optimally conduct informational-psychological operation. The method of estimation of information stability of the sociotechnical system is presented, as well as a comprehensive method of counteracting information-psychological operations, which uses vite-like and compensating memes. The structural model of the multi-level information-analytical center for comprehensive

information security management is proposed. The results of the conducted research showed the possibility of using this approach for solving the problems of evaluation and management of complex information security of the multilevel sociotechnical system.

Keywords: sociotechnical system, complex information security, information warfare, special informational operations, informational-analytic center, decision support.

I. Вступ

Методи інформаційного протиборства 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 інформаційного протиборства, які базуються на різних методах маніпулювання інформацією, використовують можливості сучасних інформаційного та кіберпростору. Ці можливості обумовлюються, в першу чергу, технологіями створення системи зв'язків між користувачами та різними об'єктами, що входять у глобальне інформаційне середовище. З урахуванням сучасних можливостей створення, зберігання та поширення інформації можна констатувати, що сучасний інформаційний та кіберпростори складають специфічну арену для проведення спеціальних інформаційних операцій (СІО). Основними характеристиками СІО є такі:

- латентність агресивних дій;
- практична відсутність людських втрат;
- можливість одночасного проведення декількох СІО;
- необізнаність опонента щодо специфіки проведення СІО;
- можливість поетапного охоплення населення (ефект ланцюжкової реакції);
- неможливість (складність) визначення опонента;
- складність (неможливість) протидії впливу;
- відсутність реваншизму.

У цей список можна додати ще одну перевагу – потреба у відносно невеликих затратах, що дозволяє проводити СІО відносно небагатим і невеликим суб'єктам інформаційної взаємодії.

Метою дослідження є побудова концептуального підходу щодо забезпечення комплексної інформаційної безпеки соціотехнічних систем (СТС).

II. Ситуаційна модель об'єкта впливу

Деструктивний інформаційний вплив, який спрямовується на вхід соціальної складової соціотехнічної (СТС) системи, може призвести до нестійкого стану всієї системи за рахунок подальшого впливу соціальної частини на технічну. Можливі різні комбінації взаємодії технічної і соціальної складових системи і, як наслідок, різні ризики потенційних деструктивних інформаційних впливів. Соціотехнічну систему можна представити:

$$STS=\{SuBSTSt,SuBSTSs\},$$

де SuBSTSt – підсистема СТС, яка представляє технічну складову системи, SuBSTSs- підсистема СТС, яка представляє соціальну складову системи.

У свою чергу, SuBSTSt може бути представлена такими ознаками: структура об'єкта, специфіка системи управління, характеристика інформаційно-телекомунікаційної системи (ІТС), технології, що використовують на об'єкті захисту, обладнання, яке розташовано на об'єкті тощо. SuBSTSs може бути представлена такими ознаками: мета впливу, розташування суб'єкта впливу, кваліфікація, доступ до спеціальних технологій, обладнання тощо.

Відповідно до новітньої термінології СІО називають кібернетичними операціями (КО) [1]. Оскільки СІО або КО, що спрямовані на СТС розраховані на ураження різнорідних складових, то доцільно їх розбити на інформаційно-психологічні операції (ІПО), що спрямовані на соціальну складову СТС та інформаційно-кібернетичні операції, які спрямовані безпосередньо на технічну складову системи.

Незважаючи на різні типи СІО сценарії їх реалізації практично збігаються і можуть бути представлені такими етапами:

- планування СІО;
- знаходження інформаційного приводу для проведення СІО;
- "розкрутка" інформаційного приводу або супровід СІО;
- вихід з процесу проведення СІО.

Наведені етапи реалізації СІО фактично представляють етапи проведення інформаційної війни.

На рис.1. представлено можливі сценарії впливу соціальної складової СТС на її технічну частину.

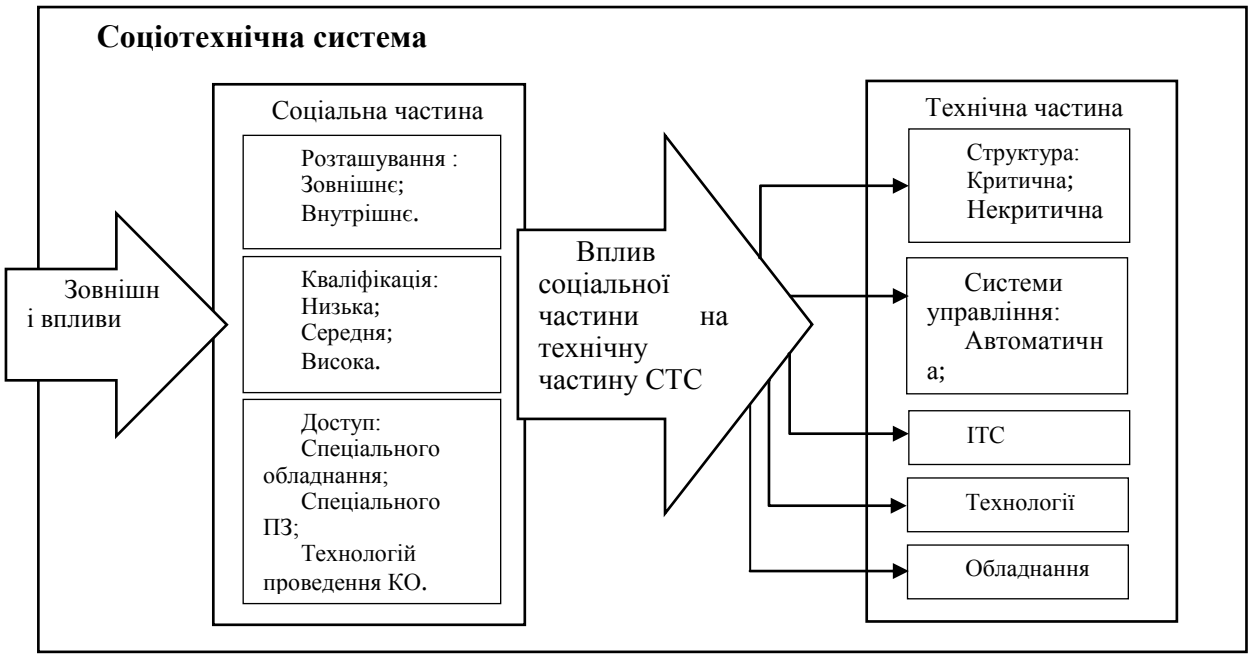

Рис.1. Сценарії впливу соціальної складової СТС на її технічну частину

У доповіді представлено низку методів та моделей, які дозволять вирішити задачі оцінювання та забезпечення гарантованого рівня комплексної інформаційної безпеки. Для розробки моделей та методів була обрана умовна одиниця інформації для впливу на свідомість людини – мем [2]. 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, зокрема запропоновано гнучкий комплексний FC-метод, що дозволяє ефективно розв'язувати задачі з комплексного захисту інформації, з урахуванням специфіки етапів проектування та експлуатації КСЗІ в умовах ведення інформаційного протиборства на рівні «підприємство–регіон–держава». Наведено метод інформаційної обфускації, метою якого є заплутування соціальної частини соціотехнічної системи. Запропоновано метод мем-програмування, метою якого є оптимальне проведення інформаційно-психологічної операції. Представлено метод оцінювання інформаційної стійкості соціотехнічної системи, а також комплексний метод протидії інформаційно-психологічним операціям, який використовує випереджувальні та компенсувальні меми.

Для практичної реалізації наведених моделей і методів запропоновано модель інформаційної підтримки та структурну модель багаторівневого інформаційно-аналітичного центру управління комплексною інформаційною безпекою на рівні «підприємство-регіон-держава».

III. ВИСНОВКИ

У представленій роботі вирішено актуальну задачу розробки концептуального підходу щодо забезпечення комплексної інформаційної безпеки соціотехнічної системи. Представлено моделі і методи проведення деструктивних інформаційних впливів та захисту від них, також запропонована структура інформаційно-аналітичного центру управління комплексною інформаційною безпекою багаторівневою СТС.

ЛІТЕРАТУРА REFERENCES

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

[2] Дудатьєв А. В. Технологии информационной войны: мем-программирование / А. В. Дудатьєв // Безпека інформації. – 2016. – Т. 23, № 1. С. 41–46.