УДК 355.01:510.21

А.В. ДУДАТЬЄВ

Вінницький національний технічний університет, м. Вінниця

ТЕОРЕТИЧНІ АСПЕКТИ ТА ТЕХНОЛОГІЇ КЕРОВАНОГО ХАОСУ ДЛЯ РЕАЛІЗАЦІЇ КОМПЛЕКСНОГО ІНФОРМАЦІЙНОГО ЗАХИСТУ СОЦІОТЕХНІЧНИХ СИСТЕМ

Анотація. Для побудови ефективної комплексної системи захисту інформації сучасної соціотехнічної системи необхідно вирішити дві задачі: захист власних інформаційних ресурсів та захист від інформаційного впливу конкурентів. 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 розглянута проблема інформаційного протиборства ймовірних конкурентів, наведена аксіоматика комплексної інформаційної безпеки соціотехнічних систем на всіх етапах їх життєдіяльності. Сформульовані і доведені теореми, які формалізують поведінку двох суб'єктів інформаційної взаємодії за певними сценаріями. Розглянуті теоретичні питання у подальшому дозволять розвинути загальну теорію комплексної інформаційної безпеки та побудувати ефективну комплексну систему захисту інформації (КСЗІ).

Ключові слова: інформаційна війна, інформаційна зброя, керований хаос, комплексна система захисту інформації.

Аннотация. Для построения эффективной комплексной системы защиты информации современных социотехнических систем необходимо решить две задачи: защита собственных информационных ресурсов и защита от информационного влияния конкурентов. Опыт последних лет и событий показывает, что эффективность применения информационного оружия в современных условиях информатизации общества достаточно велика и по своим количественным показателям сопоставима с оружием массового поражения.

В статье рассмотрена проблема информационного противоборства потенциальных конкурентов, приведена аксиоматика комплексной информационной безопасности социотехнических систем на всех этапах её жизнедеятельности. Сформулированы и доказаны теоремы, которые формализуют поведение двух субъектов информационного взаимодействия по определённым сценариям. Рассмотренные вопросы позволят в дальнейшем развить общую теорию комплексной информационной безопасности и построить эффективную комплексную систему защиты информации (КСЗИ).

Ключевые слова: информационная война, информационное оружие, управляемый хаос, комплексная система защиты информации.

Annotation..To build an effective integrated systems information protection contemporary socio-technical systems it is necessary to solve two problems: protection of own information resources and protection informacionog impact of competitors. The experience of recent years shows that the efficiency of use of information weapons in modern conditions of Informatization of the society is quite high and their quantitative indicators comparable to weapons of mass destruction.

The article considers the problem of information confrontation potential competitors, privedena axiomatics of complex safety sociotechnical systems at all stages of its life. Formulated and proved theorems which formalize the behavior of two subjects of information interaction in certain scenarios. Considered are the questions will allow to further develop the General theory of complex information security and to build effective integrated security system informatsii.

Key words: information warfare, information weapon, controlled chaos, complex system of information protection.

Вступ

Будь-який еволюційний процес розвитку складної системи, у тому числі сучасної соціотехнічної системи (СТС), супроводжується зміною протилежних станів – хаосу та порядку. При цьому стан хаосу супроводжується зміною або загибеллю структури системи, а стан впорядкованості системи — організацією або самоорганізацією її структури. Застосування технологій керованого хаосу, ефективність яких фахівцями порівнюється зі зброєю масового знищення, в останні десятиріччя набувають все більшого розповсюдження. Головною метою однієї із конкуруючих або конфліктуючих сторін, що використовує технології керованого хаосу, як це не парадоксально, для активного елемента інформаційної взаємодії, є створення дискретного процесу розвитку опонента і таким чином унеможливлення його суб'єктивного розвитку. Реалізація цієї мети надає можливість зробити процес інформаційного протиборства максимально керованим з боку активного елемента і ефективної реалізації спеціальних інформаційних операцій. Трансформуючи цю мету на життєдіяльність сучасних СТС, які є об'єктами інформаційної взаємодії і функціонують у конкурентному середовищі, головну мету можна сформулювати як завоювання лідерства на певному сегменті ринку шляхом дискредитації або знищення конкурентів. Зрозуміло, що досягнення цієї мети реалізується за допомогою спеціальних засобів та заходів ведення інформаційних війн.

Задача забезпечення комплексної інформаційної безпеки сучасних соціотехнічних систем складається із вирішення двох завдань: захисту своїх власних інформаційних ресурсів і захисту від інформаційного впливу конкурентів. З урахуванням того, що неналежне забезпечення тієї чи іншої складової комплексної інформаційної безпеки СТС може призвести до значних втрат, тобто ризики виникнення небажаних подій у СТС можуть бути значними і навіть критичними щодо подальшого існування СТС і різних інфраструктур, які забезпечують життєдіяльність СТС. Оскільки об'єкти або СТС критичного застосування є пріоритетами ймовірних конкурентів та кіберзлочинців, то стає зрозумілою актуальність забезпечення комплексної інформаційної безпеки саме з урахуванням вищесформульованих двох задач. Наприклад, критичними системами загальнодержавного масштабу є системи, які відносяться до оборонної, енергетичної, транспортної або хімічної галузей. Несанкціоноване втручання в роботу інформаційних управляючих систем, які використовуються у

вищезгаданих галузях, може привести до зупинки роботи цілих підприємств, соціальних і екологічних катастроф і навіть “паралічу” держави в цілому.

Актуальність

Забезпечення комплексної інформаційної безпеки сучасних СТС є неперервною за своїм змістом задачею, рішення якої дозволить забезпечити необхідний або достатній рівень захищеності інформаційних ресурсів об’єкта захисту. З урахуванням сучасних тенденцій життєвого циклу складних систем, у тому числі СТС, що характеризується використанням ефективних технологій інформаційних війн, актуальним є подальший розвиток загальної теорії комплексної інформаційної безпеки СТС, що дозволить у подальшому реалізувати ефективні механізми захисту щодо зовнішнього інформаційного впливу.

Мета

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.

Постановка задачі

1. Провести аналіз умов функціонування соціотехнічних систем.
2. Сформулювати теоретичний базіс для розвитку загальної теорії комплексної інформаційної безпеки соціотехнічних систем в умовах конкурентного інформаційного середовища.

Основна частина

Повний цикл життєдіяльності СТС супроводжується взаємним впливом складових системи “людина - технологічне середовище”. Будь-яка система має свою морфологію, поведінку, самоповедінку, що породжує функціональну діяльність, відповідно до цільових функцій. Опис систем можна виконувати у декількох напрямках: функціональному, морфологічному, інформаційному тощо. Оскільки ми розглядаємо питання забезпечення комплексної інформаційної безпеки, то доцільно запропонувати підхід щодо опису системи як об’єкта захисту на всіх етапах його життєдіяльності. Отже, для кожного етапу життєдіяльності СТС були запропоновані такі аксіоми: [1]

Аксіома 1. На етапі постановки задачі комплексна безпека визначається умовами експлуатації майбутньої системи і не може бути меншою допустимого рівня.

Аксіома 2. На етапі проектування рівень безпеки забезпечується тривіальними методами, засобами та заходами, які забезпечують необхідний рівень.

Аксіома 3. На етапі реалізації системи рівень безпеки забезпечується реалізацією методів, засобів та заходів, передбачених на етапі проектування.

Аксіома 4. На етапі експлуатації безпека системи забезпечується в 2 етапи:

етап оцінювання рівня поточної безпеки;

етап забезпечення необхідного рівня безпеки.

Аксіома 5. Оцінювання рівня безпеки відбувається у конкурентному середовищі, яке включає інші антагоністичні системи.

Аксіома 6. Етап експлуатації системи може супроводжуватись її знищенням антагоністичними системами або знищенням антагоністичних систем.

Аксіома 7. Етап експлуатації системи супроводжується зміною її структури або зв’язків між елементами, що впливає на рівень її безпеки.

Аксіома 8. Кожна система має закінчення життєвого циклу.

Сформульовані аксіоми дозволяють продовжити розвиток загальної теорії комплексної інформаційної безпеки соціотехнічних систем саме з урахуванням функціонуваня СТС у конкурентному середовищі і проведенні спеціальних інформаційних операцій. Процес циклічності СТС представлений на рисунку 1.

З рис. 1 видно, що життєвий цикл розвитку СТС може відбуватися у двох напрямках: перший напрямок характеризує циклічність розвитку СТС, а другий напрямок демонструє можливий шлях, який закінчується знищенням системи. З точки зору конкуруючої сторони стан комплексної безпеки СТС за першим напрямком розвитку може задовольняти конкурента лише тимчасово, а другий напрямок є оптимальним , оскільки завершується знищенням конкуруючої системи.

Керований хаос за своєю природою – це технології інформаційної війни. Технології керованого хаосу (КХ) – це новий слабоконтрольований у наш час вид інформаційної зброї для встановлення контролю над відповідними об’єктами. Використання технологій КХ спрямоване на рішення двох основних задач: зменшення чисельності конкурентів, які представляють небезпеку та послаблення або знищення конкурентів. Коли інформаційна зброя знаходиться тільки у одного з протидіючих опонентів (суб’єкт активний), то зрозуміло, що стан іншого суб’єкта (пасивного) в більшості випадків є приреченим. Будь-який процес розвитку об’єкта супроводжується зміною фаз стану цього об’єкта: стан

порядку і хаосу. Ці стани не дискретні у часі, а з'єднуються між собою перехідними процесами, які, власне, і завершуються або станом впорядкованості, або хаосу.

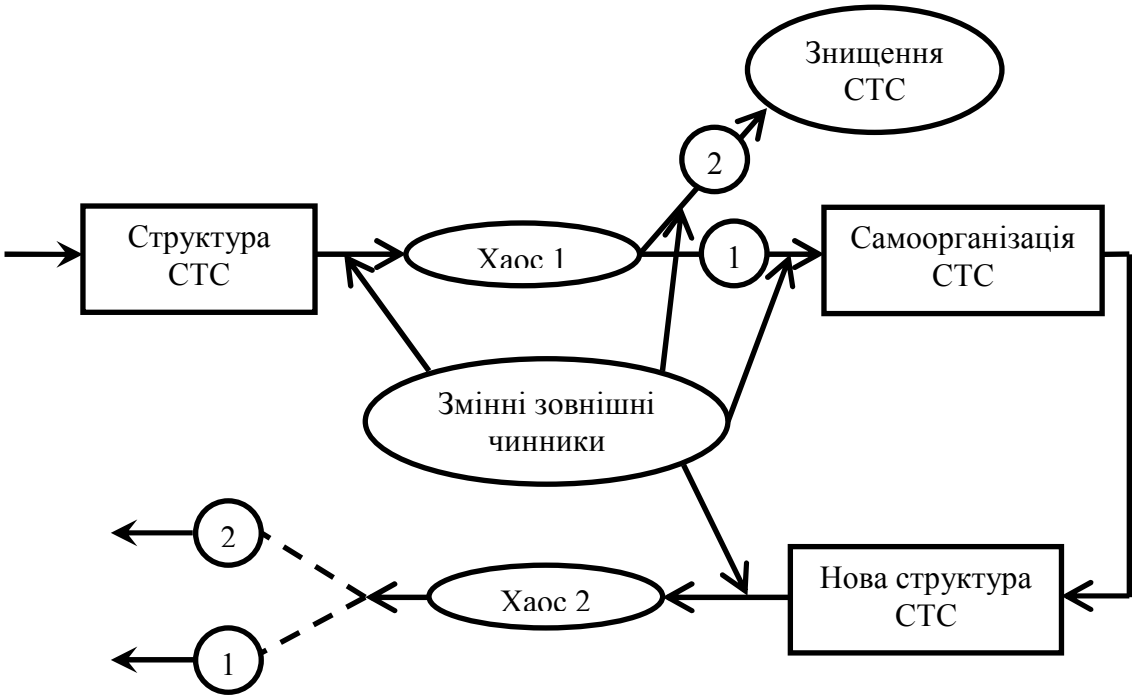

Рис. 1 – Життєвий цикл СТС

Природа хаосу може бути подвійна. Це хаос, викликаний еволюційним або суб'єктивним розвитком системи. Цей процес супроводжується зміною як структури в цілому, так і кількістю елементів та зв'язками між ними. Закінчується цей процес адаптацією системи до внутрішніх і зовнішніх змін і створенням стійкої структури. Хаос може бути викликаний також виключно зовнішнім впливом з боку конкурентів (зовнішнє середовище) з використанням спеціальних технологій ведення інформаційної війни. В будь-якому випадку, незалежно від природи хаосу, зрозуміло, що система є вразливою у режимі перехідного процесу. Саме тому спеціальні операції, які можуть бути проведені з боку конкуруючих об'єктів, є найбільш ефективними під час перехідного стану, або під час вже сформованого, або керованого хаосу. Які шляхи реалізації керованого хаосу? Ці шляхи можна узагальнити під однією назвою – «інформаційно-соціотехнічні» та ідентифікувати таким чином: нав'язування «потрібних реформ» у системі, підтримка і стимулювання запитів на штучне підвищення стандартів, знищення відповідних цінностей з метою дискредитації корпоративних секретів тощо. Реалізується керований хаос за допомогою трьох основних механізмів проведення спеціальних інформаційних операцій: механізмів реалізації пропаганди, агітації та інформаційного протиборства. Відповідно, з урахуванням можливих станів об'єктів інформаційної взаємодії (активний-пасивний) потрібно використовувати найбільш ефективні механізми проведення спеціальних інформаційних операцій. [2,3]

Виходячи з вищенаведеного і використовуючи загальносистемні визначення, сформулюємо теореми.

Теорема 1. Якщо об'єкти (суб'єкти) інформаційної протидії O_1 і O_2 взаємодіють за сценарієм «активний - пасивний», то результат проведення спеціальних інформаційних операцій для активного об'єкта може бути задовільним. $SYS_1 = \{STR_1, E_1, Z_1, P_1\}$

Доведення: Нехай об'єкт O_1 описується множиною $SYS_1 = \{STR_1, E_1, Z_1, P_1\}$, а об'єкт O_2 описується відповідно множиною $SYS_2 = \{STR_2, E_2, Z_2, P_2\}$, де STR_1, STR_2 відповідно структури для O_1 і O_2, E_1, E_2, відповідно кількості елементів для O_1 і O_2, Z_1, Z_2 відповідно зв'язки для Z_1 і Z_2, P_1 і P_2 – поведінка для O_1 і O_2. З урахуванням того, що O_1 – пасивний і виступає лише у ролі об'єкта, а O_2 – активний об'єкт взаємодії і його можна ідентифікувати, як суб'єкта інформаційної взаємодії, тобто він проводить спеціальні операції – $OPER$ над об'єктом O_1, можемо навести:

$$SYS_1 = OPER(STR'_1, E'_1, Z'_1, P'_1),$$

де STR'_1, E'_1, Z'_1, P'_1 - змінені структури, елементи, зв’язки між елементами і поведінка об’єкта O_1. Зміни, які відбуваються у пасивного елемента, а саме об’єкта інформаційної взаємодії можуть привести до зниження необхідного рівня комплексного інформаційного захисту, або навіть до знищення об’єкта, що задовольняє активний елемент, або суб’єкт інформаційної взаємодії.

Теорема 2. Якщо об’єкти (суб’єкти) інформаційної протидії O_1 і O_2 взаємодіють за сценарієм «активний-активний», то результат проведення спеціальних інформаційних операцій з обох боків не може бути задовільним.

Доведення: Нехай об’єкт (суб’єкт) O_1 описується множиною $SYS_1 = \{STR_1, E_1, Z_1, P_1\}$ а об’єкт O_2 (суб’єкт) описується відповідно множиною $SYS_2 = \{STR_2, E_2, Z_2, P_2\}$, де STR_1, STR_2 відповідно структури для O_1 і O_2, E_1, E_2, відповідно кількості елементів для O_1 і O_2, Z_1, Z_2 відповідно зв’язки для Z_1 і Z_2, P_1 і P_2 – поведінка для O_1 і O_2. З урахуванням того, що O_1 – активний елемент і виступає у ролі об’єкта і суб’єкта інформаційних відносин одночасно, і O_2 – також активний елемент інформаційної взаємодії, тобто вони проводить спеціальні інформаційні операції – $OPER$ по відношенню один до одного і комплексно захищають власні інформаційні ресурси, можемо навести:

$$SYS'_1 = OPER'_2(STR'_1, E'_1, Z'_1, P'_1),$$

$$SYS'_2 = OPER'_1(STR'_2, E'_2, Z'_2, P'_2),$$

де SYS'_1 і SYS'_2 представляють змінені структури об’єктів захисту) O_1 і O_2 .Це означає, що під дією спеціальних операцій, які використовували як суб’єкт O_1 ,так і суб’єкт O_2 , відбулися відповідні структурні зміни як у SYS_1 ,так і у SYS_2 , які не відповідають оптимальному стану елементів інформаційної протидії як об’єктів захисту.

Наведені теореми демонструють можливі шляхи розвитку сучасних СТС, які перебувають у стані інформаційної протидії і створюють теоретичне підґрунтя для розробки математичних моделей інформаційних війн.Очевидно, що ефективність інформаційного впливу визначається кількістю об’єктів, що змінили свій стан у тому напрямку, який необхідний для об’єкта впливу. Аналіз моделей інформаційних війн надасть можливість зробити попередній аналіз ризиків відносно ефективності застосовуваних джерел та механізмів проведення спеціальних інформаційних операцій і проведення ранжування відносно важливості ймовірних інформаційних спеціальних операцій і відповідно слабких місць у системі комплексного інформаційного захисту. Іншими словами, результати аналізу дозволяють визначити найбільш небезпечні як джерела, так і механізми проведення інформаційних операцій. Це дає можливість мінімізувати можливі втрати, побудувати ефективний комплексний захист інформаційних ресурсів для об’єкта захисту шляхом використання оптимального складу засобів та заходів щодо реалізації комплексного захисту.Приклад

Запропоновані теоретичні аспекти загальної теорії комплексної інформаційної безпеки розглянемо на прикладі двох сценаріїв поведінки взаємодіючих об’єктів (суб’єктів): 1-й сценарій описується ситуаційною моделлю «активний-пасивний» і другий сценарій описується ситуаційною моделлю «активний-активний». Загальним для двох сценаріїв поведінки є нав’язування певних стандартів: технологічних, інформаційних, економічних, соціальних тощо. Нав’язуваня стандартів або моделей поведінки спрямовується, в першу чергу, до використання і доступу до різноманітних ресурсів, які для об’єкта впливу можуть бути і критичними, а це означає, що для першого типу взаємовідносин інформаційний вплив може бути оптимальним для активного об’єкта. Для другого сценарію поведінки результат проведення спеціальних інформаційних операцій може бути не оптимальним або незадовільним для обох суб’єктів інформаційної взаємодії, оскільки активні дії відбуваються з двох боків. В якості прикладу можна навести відомі ситуації з реалізацією готової продукції: якщо немає вибору – то, що продається, те і купується. Зрозуміло, що під поняттям “продукція” слід розуміти все, що має соціальний попит, у тому числі і інформаційний продукт. Альтернативний варіант – вибір у покупця є і підприємство, продукція якого не реалізується (воно переможене) або поступово завершує свою життєдіяльність, або прикладає певні зусилля для своєї самоорганізації з метою подальшого виживання.

Висновки

Запропоновані теоретичні аспекти загальної теорії комплексної інформаційної безпеки сучасних соціотехнічних систем дозволяють у певній мірі формалізувати можливі варіанти або сценарії проведення інформаційного протиборства конкуруючих сторін , що у подальшому надасть можливість організувати ефективний захист безпосередньо власних інформаційних ресурсів та реалізувати захист від інформаційного впливу конкурента.

Література

1. Дудатьєв А.В. Аксіоматика комплексної безпеки соціотехнічних систем / А.В. Дудатьєв // Інформаційні технології та комп'ютерна інженерія. – 2013. -№1(26). – С. 22-25.
2. Цыганов В.В. Интелектуальные механизмы информационных войн / В.В. Цыганов, С.Н. Бухарин, В.В. Васин // Поблемы управления. – М.:, 2007. – №1. С. 25-30.
3. 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.

Стаття надійшла: 25.06.2014.

Відомості про авторів

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