УДК 004.056 DOI: 10.18372/2073-4751.74.17875

[1]Безвершенко Є.І.,
orcid.org/0000-0002-8068-1576,
[2]Гузій М.М., к.т.н.,
orcid.org/0000-0003-4807-8862

МОДЕЛІ ІНФОРМАЦІЙНИХ КОНФЛІКТІВ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ

[1]Ужгородський національний університет
[2] Національний авіаційний університет

1bezvershenko@gmail.com,
2nn05@ukr.net

Вступ

Становлення наукового напряму дослідження систем захисту інформації в умовах конвергенції телекомунікаційних та комп'ютерних мереж актуалізує проблему розробки ефективних технологій захисту інформації в інфокомунікаційних системах (ІКС). Як показує практика, впровадження сучасних технологій захисту інформації в телекомунікаційних та комп'ютерних системах (шифрування даних, процедур ідентифікації т.і.), не забезпечує захищеність обробки, зберігання і передачі інформації, оскільки відбувається адаптивне ітераційне вдосконалення засобів інформаційного протиборства та стратегій їх застосування.

Розширення інформаційного середовища взаємодії відкритих систем, впровадження ІКС в контурі управління критичними об'єктами, технологій *IoT,* хмарних технологій призводить до появи нових загроз захищеності інформації, пов'язаних із застосуванням супротивником цілеспрямований дій в умовах інформаційного протиборства та використання програмно-технічних засобів деструктивної дії.

Сучасна наукова література відображає різноманітні підходи до моделювання інформаційних конфліктів (ІК) у ІКС.

В одному з перших досліджень ІК [1] запропоновано динамічну модель інформаційних конфліктів в інтелектуальних системах. Проведено аналіз вербальних, логічних та математичних методів моделювання інформаційних конфліктів. Виконано параметричний аналіз запропонованої моделі ІК на основі розв'язку системи диференційно-логічних рівнянь.

У роботі [2] розглянуто теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор та диференціальних перетворень. Розроблено спектральні моделі процесів нападу на інформацію та запропоновано моделі їх векторної оптимізації. Висвітлено основи моделювання процесів нападу на інформацію на графах. Наведено рекомендації щодо застосування розроблених основ і наведено модельні приклади.

Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси розглянута у роботі [3]. Запропоновано методологію синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу. Створена методологія з єдиних системних позицій дозволяє здійснювати синтез диференціально-ігрових методів моделювання процесів кібернападу, які передбачають застосування комплексів відповідних моделей різного ступеню точності, від моделей оцінювання рівня захищеності – до моделей прогнозування розвитку динаміки процесу кібернападу. Застосування методології сприяє процесу інтеграції прогресивних систем інформаційної безпеки в новостворювані ІТ-технології, що, поряд з вирішенням основних завдань за призначенням, вирішують завдання інформаційної безпеки та є

стійкими до прогнозованого класу кібератак і параметрів, які їх характеризують. Результати методології відображаються як у кількісній, так і якісній формі, що не суперечить основним положенням теорії складних систем.

Результати дослідження захисту інформації в комп'ютерних системах транспортної інфраструктури наведені у роботі [4]. Проведено аналіз диференціально-ігрових моделей та методів моделювання процесів кібернападу на сервери комп'ютерних інформаційно-діагностичних систем, розроблено уніфіковану диференціально-ігрову модель процесу кібернападу на мультизадачний сервер комп'ютерної системи, отримані оптимальні стратегії захисту інформації в умовах кібератак.

Аналіз наукових публікацій показує актуальність проблеми удосконалення існуючих та розробки нових методів управління процесами захисту інформації в динамічних умовах інформаційного протиборства, необхідності розробки теоретичних основ, наукових методів і моделей управління захистом інформації в ІКС.

Мета

Метою дослідження є системний аналіз моделей інформаційного конфлікту в інфокомунікаційних системах.

Основна частина

Інфокомунікаційну систему можна розглядати як сукупність інформаційних ресурсів та алгоритмів їх обробки, що реалізовуються на основі системного та прикладного програмного забезпечення.

Інфраструктура ІКС реалізується сукупністю телекомунікаційних та інформаційно-обчислювальних систем (ТКС/ІОС).

Інформаційний конфлікт виникає при відсутності централізованого управління або наявності нерозподіленого ресурсу в доступному інформаційному просторі за наявності конфліктуючих компонентів взаємодіючих ІОС.

Під інформаційним конфліктом в даній роботі розуміється функціонування ІОС при наявності конфліктного компонента у взаємодіючих системах, виконання якого зменшує вірогідність досягнення цільових функцій ІОС.

Узагальнений інформаційний ресурс конфліктуючих систем можна представити у загальноприйнятому абстрактному вигляді як деяку безрозмірну функцію виду:

$$R=\sum_i (r_i \times W_i),$$

де w_i – деякий ресурс системи (апаратно-програмні засоби, пропускна спроможність каналу, бази даних та ін.); r_i – ваговий коефіцієнт, відносний внесок i-того ресурсу в загальний інформаційний ресурс системи.

Конфліктуючі системи за принципами побудови та функціонування умовно можна розділити на групи:

- *відкриті* – взаємодія яких з іншими інформаційними системами будується на концепції відкритих систем на основі моделі OSI;
- *закриті* (консервативні) – що працюють по незмінному протоколу з джерелами інформації та обробляють її по незмінному алгоритму;
- *гібридні (умовно відкриті/закриті)* – формально відкриті/закриті інформаційні системи, які мають в своєму складі приховані протоколи доступу та алгоритми обробки отримуваної інформації.

Моделі інформаційних конфліктів багатоаспектно відтворюють особливості реалізації конфліктного компоненту в ТКС/ІОС. Їх можна умовно розділити на підходи, що засновані на точних (алгоритмічних) моделях та підходи, які базуються на продукційних або ігрових моделях.

Перший підхід дозволяє отримати точну статичну модель конфлікту. Другий підхід враховує динаміку поведінки конфліктуючих систем.

Математичну модель інформаційного конфлікту в ТКС/ІОС можна описати загальновідомою системою рівнянь динамічної зміни ймовірностей станів конфліктуючих систем:

$$\begin{cases} P_1(X^k_{i,j}) = P_{0,1}(X^k_{i,j-1}) - \sum_{m=2}^{M}\sum_{v=1}^{V} Q_{1,m} \cdot P_{1,S}(X^v_{i,j-1}) \cdot Q_{1,R}(X^k_{i,j-1}, X^v_{i,j-1}) \\ P_2(X^k_{i,j}) = P_{0,2}(X^k_{i,j-1}) - \sum_{m=1,m\neq 2}^{M}\sum_{v=1}^{V} Q_{2,m} \cdot P_{2,S}(X^v_{i,j-1}) \cdot Q_{2,R}(X^k_{i,j-1}, X^v_{i,j-1}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P_N(X^k_{i,j}) = P_{0,N}(X^k_{i,j-1}) - \sum_{m=1,m\neq n}^{M}\sum_{v=1}^{V} Q_{n,m} \cdot P_{N,S}(X^v_{i,j-1}) \cdot Q_{N,R}(X^k_{i,j-1}, X^v_{i,j-1}) \end{cases}$$

де $P_N(X^k i,j)$ – поточна вірогідність реалізації N-ою інформаційною системою своєї цільової функції i-ою послідовністю дій для вирішення $к$-го завдання на основі j-ої сукупності даних; $P_0,N(X^k i,j)$ – початкова вірогідність реалізації своєї цільової функції N-ою інформаційною системою (або елементом); $Q_{n,m}$ – вірогідність доставки дії від n–ої інформаційної системи до m–ої системи; $P_N,S(X^v i,j)$ – вірогідність помилки реалізації цільової функції N–ою системою (компонентом) при дії i-ої послідовністю дій v–го типу інформаційної дії при j-ій послідовності початкового масиву; $Q_{N,R}$ – коефіцієнт відновлення інформаційної системи, що визначає кількість пропущених реалізацій цільової функції для відновлення початкового стану $P_0,N(X^k i,j)$ або мінімального допустимого рівня функціоналу системи.

На основі вирішення наведеної модельної задачі визначається динаміка поведінки системи при активації конфліктного компоненту.

Важлива особливість інформаційного конфлікту полягає у невизначеності використання виділеного ресурсу оперуючими системами. При дослідженні конфлікту ІОС і ТКС можна виділити наступні види невизначеності:

- невизначеність, пов'язана з неповнотою факторологічних знань про стан системи;
- невизначеність процесів, що впливають на динаміку конфлікту;
- невизначеність, яка пов'язана з невідомою оперативною поведінкою протидіючої системи.

Конфлікт ТКС протікає в послідовності чергових дій сторін (стратегій) оперуючих сторін; ІК можна представити як ітераційний процес, в якому комплекс дій кожної сторони здійснюється синхронно, формуючи функціональні цикли станів протиборчих сторін.

При системному дослідженні динаміки інформаційного конфлікту формулюються наступні завдання:

- провести аналіз взаємодії конфліктуючих систем з урахуванням існуючих зовнішніх і внутрішніх чинників (визначити зв'язки між системами, механізми функціонування, динаміку та результати взаємодії);
- виділити визначальні критерії досягнення цільової функції кожної з протиборчих систем;
- побудувати рандомізовану логічну модель динаміки інформаційного конфлікту для отримання системи логіко-диференціальних рівнянь динаміки конфлікту;
- провести параметричній аналіз моделей для виявлення причинно-наслідкових зв'язків динамічних моделей ІК та розробити їх уточнені моделі.

Моделі інформаційного конфлікту в ТКС/ІОС за типологією можна представити наступним чином:

- інформаційна модель (відображає архітектуру систему та її складові частини, інтерфейси підсистем, формат представлення даних, топологію інформаційної інфраструктури);
- функціональна модель (визначає механізм реалізації цільової функції, алгоритми управління системою та алгоритми прийняття рішень);
- морфологічна (топологічна, структурна) модель (визначає структуру ТКС/ІОС, склад і зв'язки підсистем).

Методологія дослідження взаємодії захищених інформаційних систем, що функціонують в середовищі інформаційного конфлікту, визначає взаємозв'язані етапи дослідження ТКС/ІОС.

Узагальнена схема дослідження конфліктуючих ТКС представлена на рис.

1. Постановка задачі. Аналіз ТКС/ІОС. Визначення мети та задач дослідження, цільової функції, критерів і обмежень. Побудова концептуальної моделі ІК в ТКС/ІОС.

2. Формування моделі ІК в ТКС/ІОС. Структурний аналіз ТКС/ІОС, декомпозиція системи, виділення підсистем за їх призначенням і умовами функціонування. Розробка моделі системи; представлення вибраного критерію ефективності (цільової функції) досліджуваної захищеної ТКС .

3. Розробка алгоритмів та програмного забезпечення, проведення моделювання ІК в умовах невизначеності.

4. Аналіз результатів моделювання, оцінка якості моделі, корегування моделі ІК (при необхідності, п 1,2,3).

5. Інтерпретація результатів комп'ютерного моделювання. Прийняття рішень по управлінню ІК.

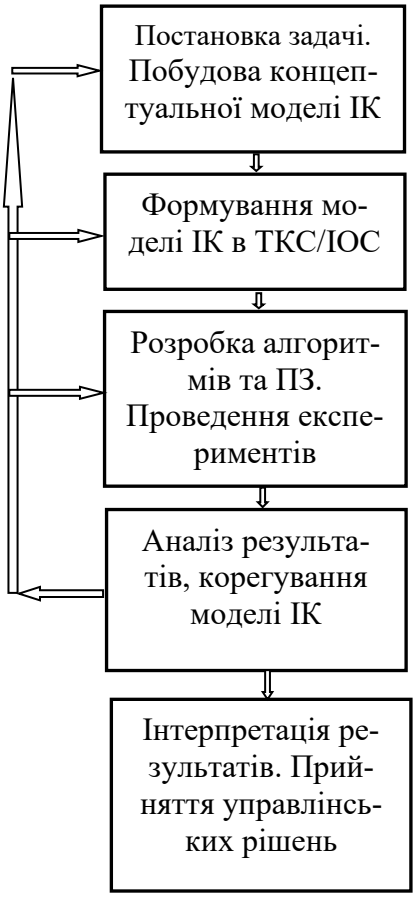

Рис. Узагальнена схема дослідження конфліктуючих ТКС

Висновки

У роботі виконано аналіз моделей інформаційної конфліктної взаємодії в інфокомунікаційних системах; розглянуто методику моделювання динаміки інформаційного конфлікту; запропоновано формалізоване представлення інформаційного конфлікту; визначено методи та етапи дослідження інформаційного конфлікту в ТКС/ІОС.

Література

1. Ігнатов В.О., Гузій М.М. Динаміка інформаційних конфліктів в інтелектуальних системах. *Проблеми інформатизації та управління*. 2005. В. 4, №15. С. 88–92.

2. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія. Житомир : Рута, 2010. 280 с.

3. Грищук Р.В. Корченко О.Г. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси. *Захист інформації*. 2012. В. 3. С.115–122.

4. Воронько І.О. Диференціально-ігрова модель захисту інформації для комп'ютерних систем транспортної інфраструктури. *Збірник наукових праць ДУІТ. Серія «Транспортні системи і технології»*. 2021. В. 38. С.201–212.

Безвершенко Є.І., Гузій М.М.

МОДЕЛІ ІНФОРМАЦІЙНИХ КОНФЛІКТІВ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ

У проведеному дослідженні виконано системний наліз моделей інформаційної конфліктної взаємодії в інфокомунікаційних системах (ІКС). Інфраструктура ІКС реалізується сукупністю телекомунікаційних та інформаційно-обчислювальних систем (ТКС/ІОС). Аналіз наукових публікацій показує актуальність проблеми удосконалення існуючих та розробки нових методів управління процесами захисту інформації в динамічних умовах інформаційного протиборства з урахуванням невизначеності інформації про дії супротивника, необхідності розробки теоретичних основ, наукових методів і моделей управління захистом інформації в ІОС. На сучасному етапі співіснують декілька підходів до моделювання інформаційних конфліктів, які відтворюють специфічні особливості реалізації конфліктного компоненту. Їх можна умовно розділити на підходи, що засновані на точному описанні, та підходи, які базуються на продукційних або ігрових моделях.

Математичну модель динаміки інформаційного конфлікту в ТКС/ІОС представлено загальновідомою системою рандомізованих рівнянь динамічної зміни ймовірностей станів конфліктуючих систем. Важлива особливість інформаційного конфлікту полягає у невизначеності використання виділеного ресурсу оперуючими системами. Визначені методологія та етапи дослідження взаємодії захищених інформаційних систем, що функціонують в середовищі інформаційного конфлікту в ТКС/ІОС.

***Ключові слова**: модель, інфокомунікаційна система, інформаційний конфлікт, методологія, інформаційна система, телекомунікаційна система, обчислювальна система.*

Bezvershenko E.I., Huzii M.M.

MODELS OF INFORMATION CONFLICTS IN INFOCOMMUNICATION SYSTEMS

In the present study, a systematic analysis of models of information conflict interaction in infocommunication systems (ICS) is carried out. The infrastructure of ICS is realized by a set of telecommunication and information-computing systems (TCS/ICS). The analysis of scientific publications shows the relevance of the problem of improving existing and developing new methods of managing information security processes in the dynamic conditions of information confrontation, taking into account the uncertainty of information about the enemy's actions, the need to develop theoretical foundations, scientific methods and models of information security management in IIS. At the present stage, several approaches to modeling information conflicts coexist, which reproduce the specific features of the conflict component. They can be conditionally divided into approaches based on precise description and approaches based on product or game models.

The mathematical model of the dynamics of information conflict in TCS/IS is represented by a well-known system of randomized equations for the dynamic change in the probabilities of states of conflicting systems. An important feature of the information conflict is the uncertainty of the use of the allocated resource by the operating systems. The methodology and stages of studying the interaction of secure information systems operating in the environment of information conflict in TCS/IOS are determined.

***Keywords**: model, infocommunication system, information conflict, methodology, information system, telecommunication system, computing system.*