**УДК 355.01**

ДУДАТЬЄВ А.В.

Вінницький національний технічний університет, Вінниця

# АКСІОМАТИКА ТЕОРІЇ КОМПЛЕКСНОЇ БЕЗПЕКИ СОЦІОТЕХНІЧНИХ СИСТЕМ

**Анотація.** У статті запропоновані базові аксіоми, які відносяться до одного з ключових показників стану соціотехнічної системи – стану її захищеності в умовах ведення інформаційної війни. Наведені аксіоми в подальшому дозволять розвинути загальну теорію комплексної безпеки соцітехнічних систем.
**Ключові слова: комплесна безпека, соціотехнічна система, інформаційна війна.**
**Аннотация.** В статье предложены базовые аксиомы, которые относятся к одному из ключевых показателей состояния социотехнической системы – состояния её защищённости. Предложенные акиомы в дальнейшем позволят разить общую теорию комплексной безопасности социотехнических системю .
**Ключевые слова: комплексная безопасность, социотехническая система, информационная война.**
**Abstract:** This article contains basic axioms which are one of the key indicators of the socio-technical system - the state of its security. Proposed in the future will akiomy express a general theory of complex socio-technical security system.
**Keywords: integrated security, sociotechnical system, information warfare.**

## Вступ

Захищенність сучасних соціотехнічних систем (СТС) залежить від того наскільки ефективно система забезпечення інформаційної безпеки реагує на існуючі загрози. Важливе значення при цьому набуває оцінка стану комплексної безпеки, з урахуванням того, що життєдіяльність СТС, як об'єкта захисту відбувається у внутрішньому і зовнішньому інформаційних середовищах.

Крім того комплексна безпека сучасних СТС складається з декількох пов'язаних між собою складових. З урахуванням того, що порушення тієї чи іншої складової комплексної безпеки СТС може призвести до значних втрат, тобто наслідки виникнення небажаних подій у системі можуть бути значними і навіть критичними щодо подальшого існування самої системи і різних інфраструктур, що забезпечують життєдіяльність СТС, то такі СТС можна віднести до так званих критичних систем.

З урахуванням можливих критичних наслідків, а також того, що СТС, яка включає в себе інформаційні системи, є важливим технологічним ланцюжком щодо отримання, оброблення, зберігання і подальшого передавання інформації, то важливим моментом є забезпечення необхідного рівня захисту її інформаційних ресурсів.

Другим важливим аспектом, який суттєво впливає на функціонування СТС, є те, що вона знаходиться під інформаційним впливом конкуруючих з нею інших об'єктів, які можуть активно використовувати сучасні технології інформаційної війни з метою заволодіння перевагою на тому чи іншому сегменті ринку. Наразі популярними активними діями є проведення конкурентної розвідки, проведення промислової розвідки, проведення «чорного» PR, тощо. Тому наведені вище факти дозволяють навести актуальне твердження сучасності: необхідно захищати власні інформаційні ресурси і захищатись від інформаційного впливу конкурентів.

## Актуальність

Ідея розвитку загальної теорії безпеки СТС полягає у побудові системної моделі, яка зв'язує суб'єкти, об'єкти і фактори, що впливають на життєдіяльність системи. Системний підхід дозволить забезпечити комплексний характер захисту і випередити дії конкурентів шляхом аналізу каналів витоку інформації, виконання спеціальних операцій щодо дій конкурентів, проведення відповідних організаційних заходів, тощо.

Життєдіяльність СТС супроводжується взаємним впливом складових: людина(її знання, вміння, психологічний стан) - технологічне середовище. Крім того, цей процес відбувається у конкурентному середовищі, тобто під інформаційним впливом інших об'єктів діяльності. Застосування технологій керованого хаоса, ефективність яких фахівцями порівнюється зі зброєю масового знищення, в останні роки набувають все більшого розповсюдження. Головною метою застосування таких технологій є унеможливлення суб'єктивного розвитку об'єкта захисту, отримання лідерства на відповідному сегменті ринку шляхом дискредитації своїх конкурентів або навіть їх знищення. Тому питання оцінювання та забезпечення комплексної безпеки сучасних СТС є надзвичайно актуальним.

Метою даної роботи є забезпечення необхідного рівня комплексної безпеки сучасних СТС, які функціонують в умовах інформаційної війни шляхом подальшого розвитку загальної теорії безпеки.

## Постановка задачі

Формулювання аксіоматики загальної теорії комплексної безпеки сучасних соціотехнічних систем.

**Рішення задач**

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 [1].

Для формулювання аксіом наведемо базові системні визначення, які наведені у роботі [2].

Визначення. Системою називається сукупність універсальних складових одиниць – елементів, які перебувають у певних співвідношеннях і зв’язках між собою, завдяки чому вони й становлять певну цілісність, неподільність, унітарність.

Далі наведемо визначення, які запропоновані Шияном А.А. і з моєїї точки зору дозволяють представити конкретну систему, як об’єкта захисту з урахуванням функціонування його у множині середовищ: інформаційному, технологічному, виробничому, навколишньому тощо.

Визначення. Функціональне середовище системи – це характерна для системи сукупність правил і параметрів (часто сформульованих у вигляді законів або алгоритмів), за якими здійснюється взаємодія (обмін, взаємовідносини) між елементами системи та функціонування (розвиток) системи в цілому.

Визначення. Елемент системи – це умовно неподільна частина системи, що самостійно функціонує. Підкреслимо, що виділення елементів (розбивка системи на елементи) – це операція, у певному сенсі, суб’єктивна. І хоча вона найчастіше повністю визначає успіх або невдачу всього дослідження, вона надзвичайно важко піддається регламентації. Як правило, таке розчленовування системи здійснюється відповідно до апріорних уявлень дослідника. І, звичайно, виділення елементів істотно залежить від постановки задачі та мети, яка стоїть перед дослідником.

Визначення. Структура системи – це сукупність «ключових» елементів, які перебувають між собою в «сильних» зв’язках, що забезпечують такий обмін інформацією між елементами системи, який є визначальним для функціонування системи в цілому та способів її взаємодії із зовнішнім середовищем. Такі «структурозадаючі» елементи є свого роду «унікальними», виділеними. Проте вони є виділеними не за своєю індивідуальною специфікою, але за їх місцем розташування та їх роллю у функціонуванні системи.

Визначення. Границя системи – це сукупність пов’язаних між собою елементів, які – взяті у своїй сукупності – дозволяють здійснювати поділ на «внутрішнє» (наприклад, функціональне середовище системи) і «зовнішнє» середовища для розглянутої системи. Через такі «прикордонні» елементи, а, точніше, «місця», які вони займають, і відбувається весь обмін інформацією між системою та її оточенням.

Важливим практичним наслідком наведених визначень є можливість ідентифікації системи з обов’язковим описом таких даних: а) універсальних складових одиниць – (функціональних) елементів системи; б) зв’язків, які існують між цими елементами; в) особливо виділити структуру системи (як сукупність «специфічних місць», потрапляючи в які елементи здобувають «особливу вагу і значення», а також систему зв’язків між такими «виділеними» місцями); г) сукупність «прикордонних» елементів (скоріше навіть тих «місць», тих положень елементів у системі, знаходження в яких і надає цим елементам здатність «відмежовувати» внутрішність системи від навколишнього середовища. І кожен із перерахованих вище 4-х пунктів потрібно описати як в статиці так і в динаміці, які формально можна представити у вигляді ситуаційних моделей. Таким чином, приходимо остаточно до опису довільної системи у вигляді восьми введених вище класів даних .

Задачу оцінювання та забезпечення комплексної інформаційної безпеки СТС будемо розглядати як наскрізну, тобто процес забезпечення безпеки необхідно реалізовувати на всіх етапах її життєдіяльності.

Для подальшого формулювання аксіоматики наведемо узагальнені ситуаційні моделі, які формалізують ймовірну поведінку об’єктів – конкурентів взаємодії під час ведення спеціальних інформаційних операцій.

Розглянемо два часткових варіанти взаємодії об’єктів. На рис.1 представлена взаємодія об’єктів А і В, яка відбувається за сценарієм – об’єкт А – пасивний, а об’єкт В – активний. Тобто об’єкт А не виконує жодних дій (протидій) по відношенню до об’єкта В.

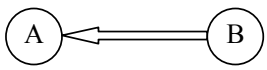


Рисунок 1 − Ситуаційна модель «активний-пасивний»

Реалізація такого сценарію може привести до змін структури і зв’язків об’єкта А, що у свою чергу дозволить об’єкту В отримати перемогу над об’єктом А.

На рис.2. представлена другий сценарій взаємодії об’єктів: об’єкт А активний і об’єкт В активний.

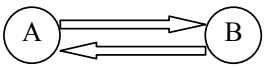


Рисунок 2 − Ситуаційна модель «активний-активний»

Реалізація другого сценарію може привести до змін структури і зв'язків, як об'єкта А так і об'єкта В. Переможець реалізації такого сценарію буде визначатися множиною чинників головними з яких є такі: наявність і кваліфікація працівників інформаційно-аналітичної служби, ефективність прогнозування розвитку подальших подій, якісне планування, спеціальне керування персоналом, координація і контроль прийнятих рішень.

Як відомо, є такі етапи життєдіяльності будь-якої системи, зокрема СТС:

- етап постановки задачі;
- етап проектування системи;
- етап створення системи;
- етап експлуатації системи;
- етап закінчення життєдіяльності системи.

Виходячи з вищевикладеного доцільно запропонувати такі аксіоми відносно кожного етапу життєдіяльності:

На етапі постановки задачі оцінювання та забезпечення безпеки формалізується такою аксіомою.

**Аксіома 1.** На етапі постановки задачі рівень безпеки визначається елементами системи, зв'язками між елементами, а також умовами експлуатації майбутньої системи і не може бути меншою допустимого рівня.

$$Z_{\tilde{n}\grave{e}\tilde{n}} \geq Z_{\ddot{a}\hat{i}\,\ddot{i}}\ .$$

де Zсист - рівень безпеки системи, що проектується, Zдоп - допустимий рівень безпеки.

На етапі проектування системи поставлена задача описується такою аксіомою.

**Аксіома 2.** На етапі проектування рівень безпеки забезпечується тривіальними методами, засобами та заходами з урахуванням умов експлуатації, які забезпечують виконання:

$$Z_{\tilde{n}\grave{e}\tilde{n}\grave{o}} \geq Z_{\ddot{a}\hat{i}\,\ddot{i}}\ .$$

Для етапа створення системи пропонується така система:

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

Етап експлуатації системи характеризується декількома аксіомами:

**Аксіома 4.** На етапі експлуатації рівень комплесної безпеки СТС забезпечується в 2 етапи:

1. Оцінювання рівня комплексної безпеки;
2. Забезпечення необхідного рівня комплексної безпеки.

**Аксіома 5.** На етапі експлуатації, оцінювання та забезпечення необхідного рівня комплексної безпеки відбувається у конкурентному середовищі, яке включає інші антагоністичні системи.

**Аксіома 6.** На етапі експлуатації системи під інформаційним впливом конкуруючої системи може відбуватися зміна її структури або зв'язків між елементами, що може привести до зменшення необхідного рівня комплексної безпеки.

$$S = (E, ST, B, Q)$$

$$S1 = F(S) = (E1, ST1, B1, Q1),$$

де S - початкова система, яка має необхідний рівень безпеки, E - елементи цієї системи, ST - структура цієї системи, B - поведінка системи, Q – середовище, у якому система експлуатується, F - оператор перетворення. Відповідно для системи S1 маємо нові параметри E1, ST1, B1, Q1, які змінені внаслідок інформаційного впливу конкуруючої системи, і які вже не забезпечують необхідного рівня безпеки.

**Аксіома 7.** На етапі експлуатації системи може відбуватися її знищення антагоністичними системами або знищенням антагоністичних систем . У такому випадку можливі 2 варіанти:

1. $Z_{\tilde{n}\grave{e}\tilde{n}\grave{o}} < Z_{\ddot{a}\hat{i}\,\ddot{i}}$,

якщо у результаті експлуатації відбулося знищення системи.

2. $Z_{\tilde{n}\grave{e}\tilde{n}\grave{o}} \geq Z_{\ddot{a}\hat{i}\,\ddot{i}}$

якщо у результаті експлуатації відбулося знищення антагоністичної системи.

Етап закінчення життєдіяльності системи описується такою загальносистемною аксіомою.

**Аксіома 8.** Кожна система має закінчення життєвого циклу.

Сформульовані аксіоми в подальшому дозволять розвинути загальну теорію безпеки складних систем, зокрема систем, які є критичними і функціонують в умовах інформаційної війни і досягти головної мети - забезпечення необхідного рівня безпеки.

**Висновки**

Рішення задачі оцінювання та забезпечення комплексної безпеки сучасних соціотехнічних систем, яка у багатьох випадках функціонує в умовах проведення спеціальних інформаційних операцій, які можуть бути або типовими або навпаки невідомими у великій мірі є унікальним. Забезпечення комплексної безпеки СТС – це забезпечення їх здатності до динамічного ефективного розвитку в умовах постійної зміни, як внутрішнього так і зовнішнього середовищ.

Запропоновані аксіоми дозволяють продовжити розвиток загальної теорії комплексної безпеки СТС і досягти поставленої мети - забезпечити необхідний рівень комплексної безпеки.

**Список літератури**

1. В.С.Харченко. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения / В.С.Харченко.– Харьков: Изд-во Национальный аэрокосмический университет им. Н.Е.Жуковского. ("ХАИ"), 2011. – 641 с.

2. Шиян А.А. Теоретико-ігровий аналіз раціональної поведінки людини та прийняття рішень в управлінні соціально-економічними системами. Монографія./ Шиян А.А. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 404 с.

Стаття надійшла: 28.11.2012.

**Відомості про авторів**

**Дудатьєв Андрій Веніамінович –** доцент кафедри захисту інформації, Вінницький національний технічний університет, (0432)598243, м. Вінниця, вул. Хмельницьке шосе 95.