DOI 10.15276/imms.v11.no1-2.15
УДК 004.89:681.324

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 1-2, pp. 15-25

УПРАВЛІННЯ КОНФЛІКТАМИ ТА ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕРЕЖІ INTERNET

В.О. Хорошко[1], М.М. Браіловський[2]

[1]Національний авіаційний університет, просп. Любомира Гузера, 1,
Київ, 03058, Україна; e-mail: professor_va@ukr.net
[2]Київський національний університет імені Тараса Шевченка,
вул. Богдана Гаврилишина, 24, Київ, 04116 Україна, e-mail: bk1972@ukr.net

У статті розглядається проблема підвищення ефективності управління конфліктами і інцидентами інформаційної безпеки в інфокомунікаційних та інформаційно-технічних системах, що функціонують на базі мережі Internet. Метою даного дослідження є пропозиція підходу до управління інцидентами і конфліктами інформаційної безпеки в мережах Internet, побудованого за принципом біоаналогів на базі штучних імунних систем. Проведений аналіз показує, що сучасні інфокомунікаційні та інформаційно-технічні системи, що функціонують на базі Internet, налічують тисячі суб'єктів, при цьому, визначальним фактором їх існування і розвитку є наявність захищеної системи обміну інформацією і системою управління конфліктами і інцидентами інформаційної безпеки. Результатами проведених досліджень є: запропонований, логічно обґрунтований і математично формалізований імунний підхід до інтелектуального управління конфліктами і інцидентами інформаційної безпеки в інфокомунікаційних та інформаційно-технічних системах, що функціонують на базі Internet; побудована узагальнена модель управління конфліктами і інцидентами, виділення цільових показників імунної системи; обґрунтований підхід з використанням узагальненої моделі управління конфліктами і інцидентами. Показана практична доцільність і прикладне значення отриманих результатів на прикладі застосування прототипу структури і функцій імунної системи управління конфліктами і інцидентами інформаційної безпеки на базі агентно-орієнтованого підходу до побудови розподілених систем. Даний підхід забезпечує динамічне адаптивне управління при виникненні нових конфліктів та інцидентів. Застосування прототипу штучних імунних систем в автоматизації та інтелектуалізації управління конфліктами і інцидентами інформаційної безпеки може дозволити досягти якісно нового рівня забезпечення та управління інформаційної безпеки в інфокомунікаційних та інформаційно-технічних системах, що функціонують на базі Internet. Крім того, в статті для оцінки функціональної безпеки Internet виділені фактори, які найбільшим чином визначають уразливість Internet.

Ключові слова: моделі управління конфліктами і інцидентами, інформаційна безпека, інформаційні системи, імунна система, біоаналогів.

Вступ

Найважливішою проблемою, що визначає темпи і майбутній розвиток Internet, стає інформаційна безпека (ІБ). Глибоке проникнення комп'ютерних інформаційних технологій (ІТ), інфокомунікаційних технологій (ІКТ), Internet в усі сфери людської діяльності і проблеми в їх захисті вимагають ширшого впровадження технологій інформаційного захисту. Вже сьогодні ІТ є тією «нервовою системою», кожної розвиненої держави в світі, яка дозволяє функціонувати іншим його підсистем. А ядром всієї інформаційної інфраструктури стала мережа Internet. В даний час мережа Internet об'єднує мільйони користувачів по всьому світі. Ці комп'ютери контролюють реальні фізичні об'єкти різного, парою критичного, типу. Таким чином, ІТ, ІКТ та Internet

стають критичними інформаційними технологіями, здатними впливати на національну безпеку держави і світу в цілому [1].

Слід враховувати, що глобальний розвиток інформаційних технологій в світі несе не тільки позитивний ефект. Їх зростання і застосування тягне за собою загрози не тільки інформаційної безпеки людей, а й істотно впливає на еволюційний розвиток людства в цілому, в тому числі і негативне. З'явилися і прогресують нові поняття в сфері безпеки. Це кіберзлочинність та кібербезпека, вірусна активність, несанкціонований доступ до інформації і кібершпигунство, інформаційні та гібридні війни.

Відчутним прояви проблеми ІБ є факт наявності зареєстрованих і виникнення нових інцидентів і конфліктів. Причому,спостережуване протягом багатьох років зростання числа інцидентів і конфліктів ІБ [2], змушує замислитися про пошук нових, кардинальних більш ефективних і, можливо, нестандартних шляхів вирішення завдання управління інцидент і конфліктами ІБ.

Це вплив ІТ, ІКТ та Internet на життя людей при збільшенні нових варіантів загроз безпеці змушує задуматися про перспективи і джерелах їх появи. Уявлення про те, що ІТ, ІКТ та Internet - породження людини, а не природи, і тому має повністю перебувати під управлінням людини, не витримує критики. Ці об'єкти сьогодні представляють собою по розмірності величезні і швидко зростаючі новоутворення, які до сих пір не зустрічалися в еволюції людини. Вони впливають на життя людей і в позитивному і негативному аспекті.

Позитивні прогнози розвитку ІТ, ІКТ та Internet в основному виходять від банкірів і фінансистів, що базуються на надіях зростання фінансового прибутку. Ряд негативних прогнозів лунають із боку фахівців в галузі ІТ і захисту інформації.

Всі ці прогнози [3] базуються на основі статистці відносно не довготривалої історії розвитку ІТ і Internet і не враховують систему популяційної складової, яка важливіша для еволюції людства в цілому.

Розвиток і еволюція інформаційної системи Internet можна порівняти з розвитком природного інформаційної імунною системою людини, яка за кількісними параметрами поки перевершує параметри розвитку ІТ і Internet.

Однак темпи зростання Internet і його вплив на еволюцію популяції людини змушують аналізувати і прогнозувати його розвиток на основі цієї аналогії.

Для оцінки впливу Internet на розвиток і еволюцію людини слід проаналізувати і порівняти кількісні характеристики еволюції інформаційних систем.

Вивчення і прогнозування розвитку Internet з позиції розвитку людства найбільш перспективне і корисно і для Internet, і для людства в цілому. Такий аналіз показує, що подальший розвиток Internet базується, в першу чергу, на організації механізмів і технологій захисту і безпеки інформації (імунології ІТ) і впровадження нових видів обміну інформацією, що відрізняються від існуючих достовірністю і якістю.

Хоча в слідстві деяких прогалин в розумінні механізмів імунної відповіді і міжклітинних взаємодій на сьогодні відсутня єдина теорія імунітету, проте теоретичні передумови біофізичних і медичних досліджень послужили поштовхом до виникнення нового напрямку в інформатиці –іммунокомп'ютернінга. Це дало можливість синтезувати прототипи штучних імунних систем (ШІС) для практичних застосувань [4].

Одним з активно досліджуваних програм ШІС є захист інформації, де природна імунна система (ІС) розглядається як джерело ідей і методів вирішення завдань ІБ. Спираючись на [5] та зробивши пошук по ряду наукових порталів Internet, на сьогодні можна виділити два загальних напрямки дослідження ШІС для ІБ:

1) імунні системи виявлення вторгнень, на базі алгоритму негативного відбору;

2) імунні системи розпізнавання нових комп'ютерних вірусів.

Однак невирішеними залишаються питання застосування імунного підходу для автоматизації та інтелектуалізації процесів управління інцидентами і конфліктами ІБ.

Мета роботи

Метою даного дослідження є пропозиція підходу до управління інцидентами і конфліктами ІБ в мережах Internet, побудованого за принципом біоаналогів на базі ШІС.

Основна частина

Internet - розрахований на багато користувачів (багатосуб'єктовий) комплекс програм, в якому існують користувачі і групи користувачів, які конкурують в частині досягнення своїх цілей, іноді суперечать цілям інших користувачів або їх груп. Частина користувачів переслідує зловмисні цілі з несанкціонованого доступу до інформації інших користувачів, що призводить до виникнення інцидентів і конфліктів.

Постійно мінливий склад програм в Internet і збільшення кількості користувачів функціонування Internet призводить до того, що неможливо передбачити заздалегідь якість функціонування, і вірогідні різні аномалії, що завершуються відмовами, які відбиваються на безпеці і виникненню конфліктів та інцидентів. Необхідно визнати принципові труднощі аналітичного оцінювання і прогнозування значень функціональної безпеки Internet внаслідок непередбачуваності прояви і наслідки загроз безпеки. Це призводить до практичної неможливості досягнення апріорних аналітичних розрахунків функціональної безпеки Internet [6,7].

Безпека Internet в більшості випадків визначається не тільки факторами заподіяння шкоди користувачу і виникненню конфліктів та інцидентів, а й можливістю реалізації цих факторів, тобто загрозами безпеці.

Загрози безпеці з точки зору використовуваних програмних продуктів визначаються їх вразливістю - наявністю в їх конструктивної реалізації місць і можливостей реалізації загроз безпеки [1,8].

Число атак несанкціонованого доступу прогнозується не менше ніж по одній атаці на комп'ютер в мережі на день. Не кожна атака призводить до її реалізації, але при планомірному дослідженні обраного для атаки в мережі Internet комп'ютера кожна невдала атака призводить до наближення до очікуваної мети, тобто до збільшення ймовірності несанкціонованого доступу.

Будь-яка атака, яка діє в мережі Internet, на кожному з наявних у розпорядженні системи захисту інформації (СЗІ) та засобів захисту відіб'ється по-різному: деякі з засобів можуть бути зруйновані повністю; деякі частково виведені з ладу, а для якихось вона виявиться безпечною. Облік цих відмінностей в результатах при запобіганні впливу атаки на засоби захисту та мережі є важливим під час моделювання будь-якої мережі і СЗІ, а також при встановленні стійкості СЗІ та ІБ [9].

Розвивається «некласичний» підхід в теорії управління, що ґрунтується на аналогіях архітектури та цілей функціонування складних технічних і біологічних систем - природних систем управління є найбільш перспективним на сьогоднішній день при формалізації інформаційних систем і мереж. У зв'язку з цим в якості базису для створення принципово нової універсальної моделі мережі були обрані основні принципи функціонування імунної системи людини [9].

Згідно [10] все біологічні системи на рівні клітин і молекул можуть розглядатися як системи обробки інформації. Але тільки нервова і імунна системи мають виняткові здібності до інтелектуальної обробки інформації, включаючи механізми розпізнавання,

ідентифікації, прийняття рішень в умовах невизначеності, навчання і асоціативної пам'яті [5].

ІС являє собою високо паралельну розподілену децентралізовану систему тимчасових колективів клітин [11], здатну до адаптивної інтелектуальної обробки інформації [4]. На даному етапі дослідження обмежимося лише розглядом основних здатностей ІС [4]: розпізнавати своїх або чужих серед величезної кількості молекулярних структур - антигенів з подальшою їх класифікацією і стимуляцією відповідних захисних механізмів. При цьому результатом розпізнавання є навчання і формування пам'яті до антигену. Знання про подібний антиген використовується при реакції на нові інфекції. Так ІС створює, вдосконалює і використовує знання про навколишній світ. Реакція на антиген може відбуватися не тільки на рівні окремих розпізнавальних одиниць, а й на громадському рівні (в залежності від рівня серйозності і способу проникнення інформації [11]). Локальні взаємодії визначають і реалізують глобальну імунну (нервову) реакцію, що в сукупності з безперервною мінливістю і адаптивністю імунної пам'яті по частоті і силі антигенних сигналів, є прикладом ефективного захисту при обмежених ресурсах.

Виходячи зі сказаного, визначимо аналогію функцій природної ІС з основними функціями, які повинна виконувати система управління конфліктами і інцидентами ІБ в мережі Internet:

- реєстрація, виявлення та оцінка серйозності подій, що мають ознаки інциденту і конфлікту, на різних стадіях їх реалізації, збору доказів для подальшого розслідування;
- ідентифікація конфліктності або інциденства на основі оперативного аналізу доказів, прийняття рішення в умовах неповної визначеності наявною інформацією і, при необхідності, генерації сигналу тривоги;
- обробка і усунення наслідків інциденту або конфлікту шляхом введення в дію відповідних ресурсів безпеки.

Міждисциплінарний підхід до вирішення завдання управління конфліктами і інцидентами ІБ обґрунтуємо методом індукції через зіставлення та узагальнення фактів виникнення інцидентів і конфліктів інформаційних процесів, які мають місце в системах самої різної природи від інфокомунікаційних та інформаційно-технічних (ІТС), які є складовою частиною Internet, і до біологічних [8-11].

Тому, іммунокомп’ютерінг стосовно до управління інцидентами і конфліктами ІБ в ІКС і ІТС, які функціонують на базі Internet, реалізуються з урахуванням постулатів еволюційної теорії [12]:

- доцільність: «виживають» лише ті ІКС і ІТС (елементи Internet), які найбільшою мірою відповідають ситуації, тобто пристосовуються до інцидентів і конфліктів;
- адаптація: архітектура комплексної системи інформаційної безпеки повинна дозволяти динамічно адаптуватися до нових конфліктів і інцидентів, а також до зовнішніх атак;
- самоорганізація: процес еволюції ІКС/ІТС (елементи Internet) призводить до безперервного вдосконалення її структури в зв'язку з перерозподілом ресурсів.

Розглянемо міждисциплінарну декомпозицію властивості безпеки абстрактної системи і взаємопов'язаних з нею понять, а також процесів управління і обробки конфліктів та інцидентів для наступних типів (рівнів) систем: біологічних, ІКС, ІТС та елементів Internet. Завдання управління конфліктами і інцидентами в абстрактній системі є недостатньо формалізованою і невизначеною з точки зору генної структури організації систем і мереж через недостатню розробку більш загальної (в порівнянні з класичною) теорії систем.

Так як кожна ІКС і ІТС включає підсистему ІБ, то математична модель необхідна також для управління інцидентами і конфліктами із залученням сучасного апарату теорії моделювання і складних систем [13,14], а також процесу відбиття атак.

Тепер розглянемо аналогію архітектури та цілей функціонування імунної системи людини з мережею Internet включаючи СЗІ.

При цьому використання імунної системи людини для моделювання ІКС і ІТС (елементів Internet) випливає з очевидною аналогії між обраною біологічною системою і системою ІБ. Слід враховувати, що процес моделювання тут носить комплексний характер і використовує імунну систему, починаючи з форми представлення інформації, програмування інформаційного простору і закінчуючи архітектурою елементів Internet (ІКС і ІТС) з вбудованими механізмами забезпечення ІБ і еволюційного перебігу процесів [9].

Моделювання захищених інформаційних процесів засноване на єдності подання інформації в ієрархії ІС, в якому повідомлення представляється певним структурним інформаційним полем ДНК. Структурований характер мають розподілене інформаційний простір нейронних комплексів ІС, завдяки яким в ІС існує адаптивні механізми пам'яті, які накопичують життєвий досвід. Можливість реалізації адаптивних механізмів пам'яті в штучному інформаційному просторі - основна передумова еволюції Internet. Програмування в ІС носить надлишковий розподілений характер, що забезпечує високу функціональну стійкість інформаційних процесів.

Окремі спотворення інформації, з одного боку, компенсують надмірність інформаційного простору, а з іншого - дозволяють реалізувати механізм мутацій і еволюційні процеси розвитку і відбору. Адаптивні процеси в інформаційному просторі дозволяють Internet розвиватися і накопичувати досвід в умовах розширення загроз, а успадкування досвіду в наступних реалізаціях мережі і системи зводиться до передачі відповідних інформаційних просторів. Ієрархія адаптивної системи ІБ відображає поділ функцій захисту на керуючу і керовану реалізовує взаємодії системи з середовищем (рис.1) [9]. Архітектурною особливістю ІС є внутрішній характер механізмів захисту, що реалізується в ієрархії елементів Internet.

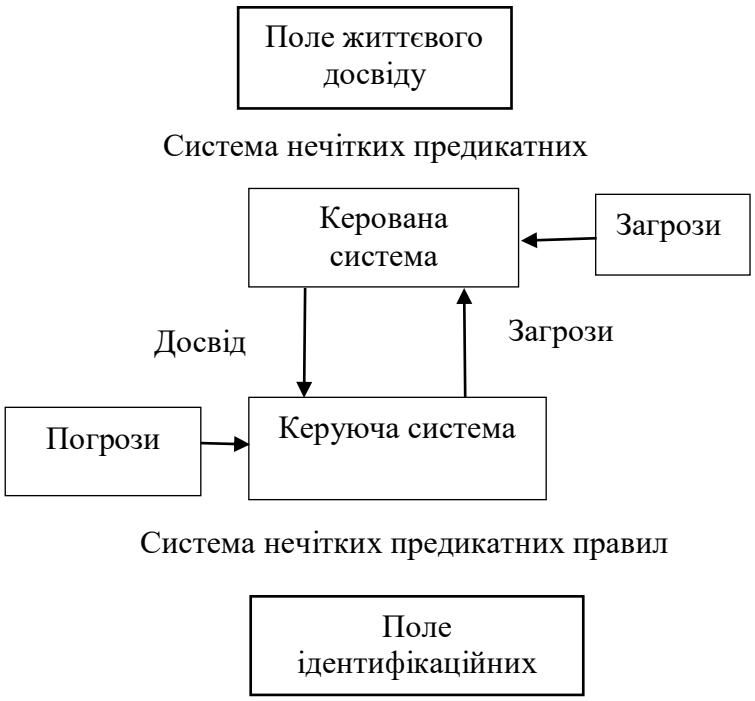

Рис. 1. Ієрархія адаптивної системи ІБ.

При моделюванні штучних систем слід враховувати, що при реалізації адаптивних механізмів ІС та інформаційного простору її функції захисту інформації повинні бути внутрішніми функціями системи.

На основі проведених досліджень приступаємо до розробки узагальненої моделі управління конфліктами і інцидентами.

Застосовуючи формалізм теорії систем [14,15], побудуємо узагальнені моделі систем, які відповідають наступним типам:

1. Для біологічної системи:

$$BioSys = (GN, EC, MB, EV, FC, RP), \quad (1)$$

де GN - генетичне початок;
EC - умови існування;
MB - метаболізм;
EV - еволюція;
FC - функціонування;
RP - репродукція.

2. Для інформаційної системи:

$$ICSys = (IR, EN, TR, CN, QS, SV), \quad (2)$$

де IR - інформаційні ресурси;
EN - середовище;
TR - телекомунікаційні ресурси;
CN - контроль, експлуатація, проектування;
QS - якість;
SV - надійність.

3. Для інформаційно-технічних систем:

$$STSys = (RI, RO, EX, MN, EF, ED), \quad (3)$$

де RI - внутрішні ресурси;
RO - зовнішні ресурси;
EX - виконавці;
MN - менеджмент, реінжиніринг;
EF - ефекти;
ED - навчання, передача знань.

Параметри GN, IR, RI є «вхідні сигнали» кожної з систем; EC, EN, RO - непередбачувані «перешкоди» (зовнішні фактори і загрози); MB, TR, EX - «оператори перетворення» (внутрішні процеси); EV, CN, MN - «зворотний зв'язок» (процеси внутрішнього розвитку і самоорганізації); FC, QS, EF - «сигнал на виході» кожної з систем (критерії ефективності «цільові процеси»); RP, SV, ED -«закінчення циклу»(відтворення, забезпечення переходу до наступних епох життя системи,«новий виток спіралі»).

Можна відзначити паралелі між параметрами моделей кожної з систем. Це підтверджується і в роботах [4,5,10,11,12,15] до розвитку природи і суспільства.

Так само ці питання вирішуються і в дослідженнях [16,17], де показано, що проблема ІБ з точки зору онтології предметної області та математичних моделей представлення знань структурно подібна проблеми захисту біологічних організмів від патогенних факторів.

При цьому слід враховувати, що інформація, що обробляється в ІКС і ІТС, які функціонують на базі Internet, особливо вразлива. Суттєвого підвищення можливості

несанкціонованого використання або модифікації даних, введення в оборот неправдивої інформації в даний час сприяють:

- збільшення обсягу інформації, що обробляється, передається та зберігається;
- зосередження в базах даних інформації різного рівня важливості і конфіденційності;
- розширення доступу кола користувачів до інформації та до ресурсів мережі, що призводить до виникнення конфліктів та інцидентів;
- збільшення числа віддалених робочих місць;
- широке використання для зв'язку користувачів мережі Internet і різних каналів зв'язку;
- автоматизація обміну інформацією між комп'ютерами користувачів.

Тому при розгляді конфліктів та інцидентів необхідно враховувати їх характер та можливості управління ними. При цьому, слід враховувати сучасні підходи до управління з розумінням існуючих підходів і особливостей ІС [11,18,19].

Відповідно до мети дослідження принцип біоаналогів і «організменого підходу», система управління конфліктами і інцидентами ІБ включаючи підсистему виявлення вторгнення (IDS) в рамках комплексної системи інформаційної безпеки (КСІБ) і ІКС і ІТС, що функціонують на базі Internet, повинні грати ту саму роль, що і імунна система в живому організмі.

Стосовно до управління конфліктами і інцидентами ІБ це повинно означати перехід від «механізму» до біологічної аналогії, коли система розуміється як така, що розвивається і розуміється крізь призму еволюційної теорії [4,8,11,19].

На підставі проведених досліджень побудуємо узагальнену модель системи управління інцидентами і конфліктами:

$$IMSys = (INC, SEC, CRI, KBS, X, Y, S, DMF, AGT, ARS, TRS, IRS, MST, T, SYN) \quad (4)$$

де INC - управління інцидентами;
SEC - безпека (мета);
CRI - критерії оцінки стану безпеки;
KBS - база знань про конфлікти і інциденти;
X - вхідні впливу;
Y - реакція на конфлікт або інцидент;
S - стан системи;
DMF - функція прийняття рішень (реагування), яка включає два підетапи: прийняття рішення про включення елемента ARS в набір TRS, і потім, на підставі першого підетапу - прийняття рішення про включення елемента ARS в набір TRS;
AGT - агенти, безліч програмно реалізованих мобільних інтелектуальних агентів;
ARS - агентно-орієнтований набір ресурсів ІБ, тобто безліч всіх доступних для агентів ресурсів безпеки;
IRS - інцидентно-орієнтований і конфліктно-орієнтований набори ресурсів безпеки, тобто підмножина ресурсів, якими володіє агент, і які в сукупності є достатніми для ефективного реагування на конкретний тип конфлікту або інцидент;
TRS - тестовий набір ресурсів безпеки, тобто підмножина ресурсів, які відбирають для імітаційного моделювання прогнозу і адаптації до невідомого типу конфлікту або інциденту;
MST - стратегія управління конфліктами і інцидентами;
T - час;
SYN - самоорганізація.

Створення та розробка методології побудови адекватних систем захисту інформації та управління конфліктами і інцидентами ІБ виходить з принципу подібності механізмів ІБ і імунної системи. При цьому, завданням, що вирішується є

розробка імунної системи управління конфліктами і інцидентами ІБ в складі СЗІ з використанням, як окремих інтелектуальних підходів, так і їх комбінацій для забезпечення розв'язуваної задачі в умовах високої динаміки загроз. Підходи до ІБ та управління конфліктами і інцидентами ІБ в такий вимірювальній системі, повинні володіти новими методами і властивостями, аналогічними зокрема методами збереження живучості (працездатності) біологічної популяційної системи живої природи.

Неодмінним властивістю будь-якої системи є наявність структури, яка представляє собою побудову системи, що відображає найбільш суттєві взаємозв'язки між елементами і їх групами (підсистемами), які мало змінюються при змінах в системі і забезпечують стале функціонування системи і її основні властивості.

У мережевої та організаційної архітектурі мережі Internet і її елементів ІКС і ІТС виділимо підсистему автоматичного управління конфліктами і інцидентами ІБ.

При цьому слід враховувати, що для забезпечення і аналізу ІБ необхідно оцінювати напрямок діяльності СЗІ, а для досягнення ефективності в її роботі доцільно виділити наступні напрямки [20]:

- захист об'єкта (мережі та її елементи);
- захист процесів або процедур обробки і зберігання інформації;
- захист каналів зв'язку;
- контроль і управління СЗІ.

Крім цього необхідно усвідомлювати, що конфлікти в мережі можуть виникати при зверненні двох і більше користувачів до одних і тих же ресурсів, каналів зв'язку, тощо. При цьому, інциденти можуть бути як зловмисними, так і випадковими (наприклад, бути наслідком помилки або природних явищ) і можуть виникати в слідстві як технічних, так фізичних засобів. Їх наслідками можуть бути такі події, як несанкціоновані зміни інформації, її знищення або інші події, які роблять її недоступною, нанесення шкоди користувачам [21].

Отже, можемо наразі приступити до побудови системи управління конфліктами і інцидентами ІБ використовуючи імунно-мультиагентну технологію [12,15,17].

Розглянемо 4 класу агентів (рис.2): агенти-детектори; агенти-ідентифікатори; агенти-координатори та агенти-реактори.

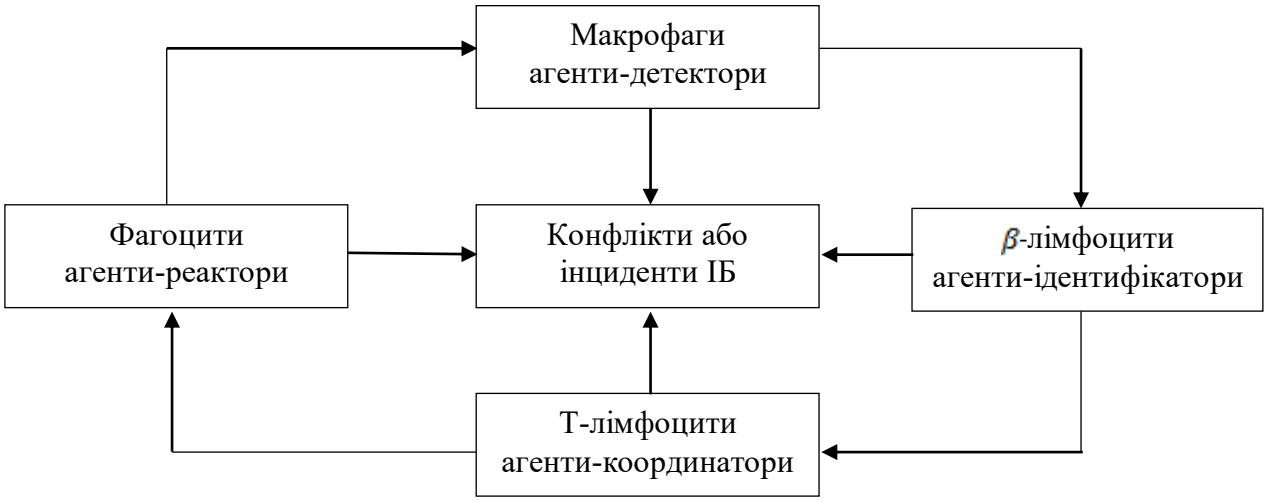

Рис. 2. Цикл і функції управління конфліктами і інцидентами за допомогою ШІС

При цьому, агенти-детектори (рецептори) - відповідають макрофагам і іншим антиген-презентируючим клітинам, які виділяють частки антигену на своїй поверхні, привертаючи увагу β-лімфоцитів для розпізнання. Агенти-ідентифікатори відповідають β-лімфоцитам, які розпізнають антиген і заздалегідь піддавалися «негативного відбору»

в тимусі. Агенти-координатори відповідають лімфокінам, які виділяються Т-лімфоцитами для активізації β-лімфоцитів. Агенти-реактори відповідають фагоцитам, які мають антитіла для знищення антигену.

Сформулюємо наступні етапи управління конфліктами і інцидентами за допомогою ШІС:

1 етап. Індикація агентами-детекторами будь-якої підозрілої активності.

2 етап. Розпізнавання агентами-ідентифікаторами ненормальної активності, як певного типу конфлікту або інциденту, за умови знаходження в базі знань відповідної сигнатури або виявлення аномалій по відношенню до еталону поведінки.

3 етап. Отримання підсистемою реагування на сигнал від IDS про ідентифікований відомий або невідомий конфлікті або інцидент.

4 етап. Ідентифікація атакуючого набору загроз конфлікту або інциденту за умови наявності у базі знань кореляції між характеристиками отриманого сигналу про конфлікті або інцидент і записами про набор атакуючих загроз.

5 етап. Формування текстових наборів механізмів захисту згідно з алгоритмом, який генерується базою знань.

6 етап. Імітаційне моделювання ефективності перекриття текстовим набором механізмів захисту - набору атакуючих загроз конкретного ідентифікованого конфлікту або інциденту.

7 етап. Прийняття рішення щодо вибору конфліктно-орієнтованого або інцидентно-орієнтованого набору механізмів захисту.

8 етап. Видача підсистемою обробки сигналу, що управляє агентом-реактором щодо обробки конфлікту або інциденту за допомогою конфліктно-орієнтованого і інциденто-орієнтованого набору механізмів захисту.

9 етап. Самоорганізація та оцінка підсистемою зворотного зв'язку і агентами-детекторами ефективності використання конфліктно-орієнтованого або інцидентно-орієнтованого набору механізмів захисту, поповнення баз знань новим досвідом, розслідування та аналіз конфлікту і інциденту, вироблення керуючого сигналу щодо превентивних дій.

Для того, щоб скласти єдиний організм агенти повинні забезпечити гомеостатичне регулювання мережі Internet в цілому та в її елементах ІКС/ІТС. Під гомеостатичним регулюванням розуміється управління конфліктами і інцидентами, що підтримує цільові характеристики мережі Internet і її складових частин ІКС/ІТС, в межах, що забезпечують її безпеку, якість, надійність і живучість.

Безпека Internet як комплексу ІКС/ІТС визначається мінімізацією вразливостей елементів Internet (ІКС/ІТС) і ступенем захищеності мереж, що функціонують на базі Internet, а також системами управління конфліктами і інцидентами ІБ.

Висновки

Проведений аналіз показує, що сучасні ІКС і ІТС, що функціонують на базі Internet, які налічують тисячі суб'єктів, визначаються фактором їх існування та розвитку, наявністю захищеної системи обміну інформацією і системою управління конфліктами і інцидентами ІБ.

Отримані науково-технічні результати: запропоновано, логічно обґрунтований і математично формалізовано імунний підхід до інтелектуального управління конфліктами і інцидентами ІБ в ІКС і ІТС, що функціонують на базі Internet; побудована узагальнена модель управління конфліктами і інцидентами. Показана практична доцільність і прикладне значення отриманих результатів на прикладі застосування прототипу структури і функцій імунної системи управління конфліктами і інцидентами ІБ на базі агентно-орієнтованого підходу до побудови розподілених систем. Даний підхід забезпечує динамічне адаптивне управління при виникненні

нових конфліктів та інцидентів. Застосування ШІС в автоматизації та інтелектуалізації управління конфліктами і інцидентами ІБ може дозволити досягти якісно нового рівня забезпечення та управління ІБ в ІКС і ІТС, що функціонують на базі Internet.

Список літератури

1. Осовецкий Л.Г. Геном информатизации и корпоративная иммунология интернета. *Системы управления связью и безопасность*.2016. № 1. С. 191-205
2. Howard J. An Analysis of Security Incidents in the Internet, *CERT//CC*, 2000
3. Осовецкий Л.Г., Немолочнов О.Ф., Твердый Л.В., Беляков Д.А. Основы корпоративной теории информации. СПб: СПбГУ ИТМО, 2004. 252 с.
4. Искусственные иммунные системы и их применение / под ред. Д. Дасгупты. М.: Физмат, 2006. 344 с.
5. Марчук Г.И. Математические модели в иммунологии. М.: Наука, 2011. 314 с.
6. Звонов Д., Нестерчук Ф.Г., Осовецкий Л.Г. К оценке защищенности корпоративной сети. НТВ *Информационных технологий, механизмов и оптики*, 2018. Т. 6, № 2. С. 156-167.
7. Осовецкий Л.Г., Суханов А.В., Ефимов В.В. Меры по обеспечению безопасности и защиты информации для сложных информационных систем. *Системы управления связи и безопасности*, 2017. № 1. С. 16-25.
8. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236 с.
9. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности. К.: ГУИКТ, 2009. 251 с.
10. Караулов, А.В. Иммунитет и инфекционные заболевания: от вакцинации к иммунореабилитации. *Практикующий врач*. 2006. № 3. С. 4-6.
11. Петров Р.В. Иммунология. М.: Медицина, 2007. 436 с.
12. Осовецкий Л.Г., Нестерчук Г.Ф., Бормотов В.М. К вопросу иммунологии сложных информационных систем. *Приборостроение*, 2003. Т. 46, № 7. С. 34-40.
13. Томашевский В.М. Моделювання систем. К.: BHV, 2007. 352 с.
14. Вунш Г. Теория систем. М.: Сов. Радио, 1978. 288 с.
15. Гладыш С.В. Применение принципа биоаналогий для синтеза систем интеллектуального управления безопасностью телекоммуникаций. *Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине*. 2006. Вип. 1 (13), С. 57-63.
16. Нестерчук Г.Ф., Осовецкий Л.Г., Нестерчук Ф.Г., Воскресенский С.И., Грибачев В.П. Информационная избыточность нейронечетких средств обеспечения безопасности. *Вопросы защиты информации*. 2003. № 3 (70), С. 12-16.
17. Нестерчук Г.Ф., Осовецкий Л.Г., Харченко А.Ф. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов (иммунология систем информационных технологий). СПб.: Гос. ун-т. экономики и финансов, 2003. 364 с.
18. Постон Т. Стюарт И. Теория катастроф и ее приложения. М.: Мир, 1980. 608 с.

19. Єжова Л.Ф., Корченко А.О., Мачалін І.О., Скачек Л.М., Хорошко В.О. Управління інформаційною безпекою. В 2-х томах. К.: НАУ, 2012.
20. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах. К.: Арий. 2008. – Том. 2
21. Капустян М.В., Олешко Т.И., Хорошко В.А. Модели передачи информации с учетом обнаружения, недопущения и устранения тупиковых ситуаций. *Вісник ДУІКТ,* 2006. Т. 4, № 3, С. 156-162.

INFORMATION SECURITY CONFLICTS AND INCIDENTS MANAGEMENT ON THE INTERNET

V.O. Horoshko[1], M.M. Brailovskyi[2]

[1]National Aviation University, Lubomyr Guzar Ave, 1, Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net
[2]Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna Street, 24, Kyiv, 04116, Ukraine;e-mail: bk1972@ukr.net

The article deals with the problem of improving the efficiency of managing the conflicts and incidents of information security in infocommunication and information technology systems operating on the basis of the Internet. The aim of this study is to propose an approach to the management of incidents and conflicts of information security in Internet networks, based on the principle of biosimilarity within the artificial immune systems.The analysis shows that the factor determining the existence and development of modern infocommunication and information technology systems, operating on the basis of the Internet and numbering thousands of entities, is the presence of a secure information exchange system and a system for managing conflicts and incidents.The results of the research are as follows: a logically grounded and mathematically formalized immune approach to the intelligent management of conflicts and incidents of information security in infocommunication and information technology systems operating on the basis of the Internet is proposed; a generalized model for managing conflicts and incidents highlighting the target characteristics of the immune system has been elaborated; an approach using a generalized model of conflict and incident management has been substantiated. The practical feasibility and significance of the results obtained is illustrated by using a prototype of the structure and functions of the immune system for managing conflicts and incidents of information security on the basis of an agent-based approach to building distributed systems. This approach provides a dynamic adaptive management in the event of new conflicts and incidents. The use of artificial immune systems in the automation and intellectualization of management of conflicts and incidents of information security may allow to achieve a qualitatively new level of provision and management of information security in information and communication systems functioning on the basis of the Internet. In addition, the article identifies the factors that have the greatest impact on determining the vulnerability of the Internet with a view to assessing the functional security of the Internet.

Keywords: conflict and incident management models, information systems, information security, immune system, biosimilarity.