УДК 681.3

Кононович В. Г., Гладиш С. В.
Kononovich V. G., Gladysh S. V.

МОДЕЛЬ МУЛЬТИАГЕНТНОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ

A MODEL OF MULTIAGENT INFORMATION SECURITY SYSTEM IN TELECOMMUNICATION NETWORK

Анотація. Розроблено моделі мультиагентної системи інформаційної безпеки в телекомунікаційній мережі. Як тестовий зразок для моделювання запропоновано схему мультиагентної системи керування міжмережними екранами.

Summary. Models of multi-agent information security system in telecommunication network are developed. A scheme of multi-agent control on firewalls is proposed as a test example for modeling.

Моделювання процесів забезпечення інформаційної безпеки (ІБ) в телекомунікаційних мережах (ТМ) є загальною проблемою, яка постає під час створення систем інформаційної безпеки (СІБ). Класифікація, аналіз та деякі підходи до моделювання процесів та систем захисту інформації досліджено в роботах [1 … 4]. Більшість цих моделей орієнтовано на традиційні технології забезпечення ІБ. Новою парадигмою створення розподілених СІБ є мультиагентні системи (МС) [5, 6], які можуть проводити аналіз захищеності комп'ютерних мереж [7], контролювати віддалені системи на предмет своєчасного накладення коригувальних латок і відсутності ознак шкідливої активності [8], виявляти розподілені, скоординовані атаки [9, 10], вносити в захист елементи динамічності та самоорганізації [11]. У [12] сформульовано підхід до моделювання протиборства зловмисників та СІБ у вигляді антагоністичної взаємодії команд програмних агентів.

Однак для ТМ завдання моделювання мультиагентних систем інформаційної безпеки (МСІБ) поки що не враховують особливості ТМ як складного об’єкта захисту (глобально-розподілений характер; велику довжину ліній зв’язку, що знаходяться на неконтрольованій території; особливі загрози, вимоги; відмінності в нормативних документах).

Метою даного дослідження є розробка моделей МСІБ ТМ, які будуть враховувати зазначені вище особливості.

Одним із основних технічних засобів захисту інформації у ТМ є міжмережний екран (МЕ, брандмауер, firewall). Наприклад, моделі Cisco Secure PIX [13] працюють під керуванням операційної системи Cisco PIX OS. Вони використовують два або більше мережних інтерфейсів, відімкнених до різних сегментів ТМ. Відповідно до правил фільтрації (ПФ), сформованих адміністратором безпеки, здійснюється розмежування доступу суб'єктів з одного сегмента ТМ до об'єктів іншого сегмента ТМ. За коректного настроювання ПФ МЕ забезпечує захист ТМ від зовнішніх та деяких внутрішніх загроз. Однак така схема має серйозні недоліки, головним з яких є складність керування політикою інформаційної безпеки (ПІБ) через розподілений характер мережі. Крім того, загальним недоліком більшості МЕ є пасивна система реагування на виявлені атаки.

В даній роботі пропонується система керування міжмережними екранами, заснована на використанні мультиагентної технології, основним завданням якої є підвищення ефективності керування ІБ шляхом уведення елементів штучного інтелекту у відповідні алгоритми. Принцип функціонування дії МС ґрунтується на розподілі загального завдання на низку взаємозалежних локальних завдань, плануванні колективної поведінки агентів, координації взаємодії агентів. У наслідок декомпозиції розв′язання загального завдання розподіляється між спеціалізованими автономними агентами. Кожний агент можна розглядати як інтелектуальний об'єкт із власною базою даних і знань, здатний адаптуватися до заздалегідь невідомих умов функціонування в середовищі з перешкодами. Методи навчання та адаптації агентів використовують моделі віртуальної реальності, які дозволяють: а) моделювати у віртуальному просторі агента навколишнє середовище та поведінку інших агентів; б) розпізнавати у віртуальному просторі ситуації та приймати оптимальні рішення. З доданням зазначених вище механізмів взаємодії агентів до типової стандартної схеми підмикання МЕ [13], розроблено таку структурну схему МСІБ (рис. 1).

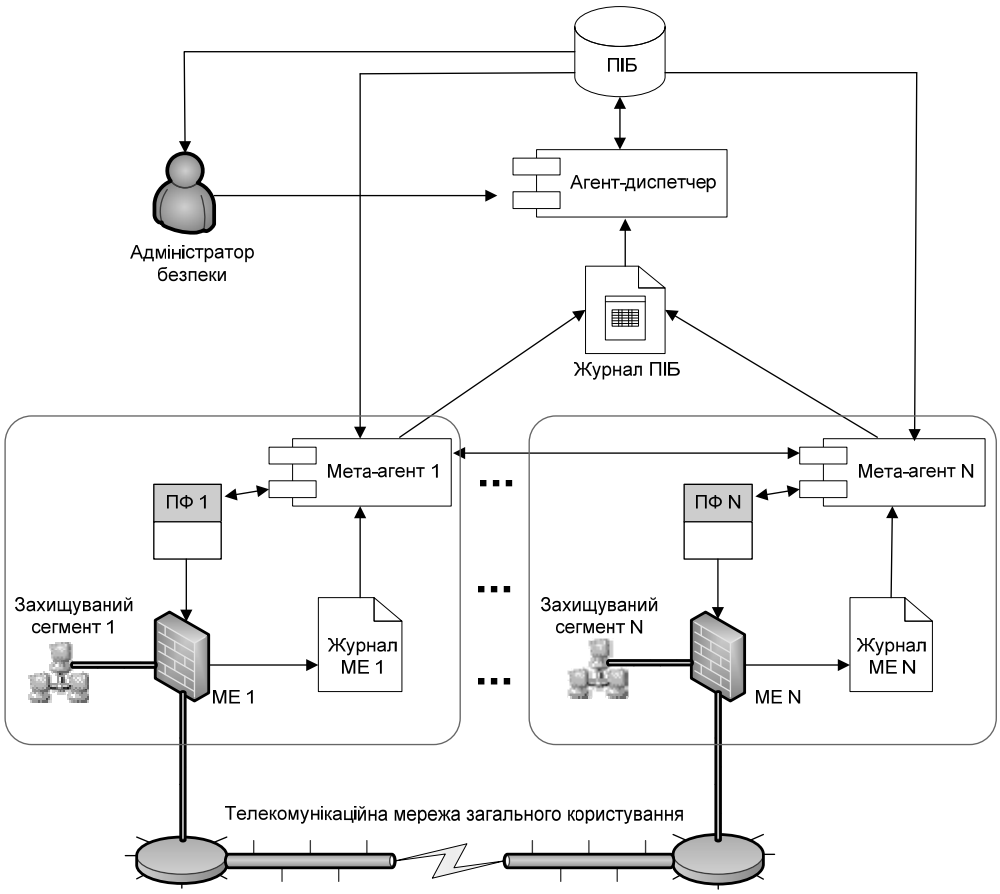

Рисунок 1 - Структурна схема мультиагентної системи керування міжмережними екранами

Система складається з наступних компонентів:

- МЕ, установлені на вузлах, що об'єднують різні сегменти ТМ;
- мета-агенти, що здійснюють керування окремим МЕ;
- агент, що приймає рішення про зміну загальної ПІБ (у масштабах усієї ТМ) і, за необхідності, виконує взаємодію з системою керування ТМ.

Виконавчий рівень системи представлено мета-агентами, які, розміщуються у вузлах ТМ та контролюють стан інформаційних ресурсів, які підлягають захисту. Мета-агент розміщується в операційній системі вузла у вигляді системного процесу та контролює всі засоби і функції ІБ, що реалізовані в програмних і апаратних засобах вузла. Мета-агент має вбудовані інтерфейси до засобів ІБ, що не дає йому можливість не тільки використовувати їх як сенсори стану вузла, але й керувати ними. Мета-агент фіксує у журналі події, що потенційно впливають на ІБ або безпосередньо, або через засоби ІБ, і передає відомості щодо них до бази даних агента-диспетчера.

Агент-диспетчер аналізує події та визначає ступінь відповідності реалізованих функцій ІБ щодо установленого у ПІБ. У випадку повної відповідності вимогам ПІБ диспетчер формує цифровий підпис (сертифікат), що підтверджує захищеність сегмента ТМ.

МЕ може гарантувати певний рівень захищеності тільки за умов коректного настроювання правил фільтрації (ПФ). Проте кваліфікації користувача може виявитись недостатньо для правильного настроювання МЕ. Некоректно настроєний МЕ – це потенційна вразливість у системі захисту ТМ. Тому доцільно автоматизувати процедуру настроювання ПФ МЕ за допомогою програм-агентів, які відповідно до ПІБ настроюють ПФ кожного окремого МЕ. Концепція програм-агентів передбачає наявність реактивності, тобто здатності сприймати середовище й адекватно реагувати на зміни, що відбуваються. Агент у реальному часі робить аналіз журналу повідомлень МЕ. При виникненні будь-якої неординарної ситуації агент може прийняти рішення щодо зміни ПФ на конкретному МЕ. Агент також може обмінюватись інформацією з іншими агентами. Всі повідомлення, що надходять від агентів, реєструються в журналі безпеки ТМ. Аналіз цього журналу в реальному часі виконує агент керування ПІБ ТМ, який працює на верхньому рівні ієрархії агентів. На

підставі отриманих даних агент може прийняти рішення про зміну ПІБ. Крім того, на дане рішення може вплинути адміністратор безпеки ТМ. Структуру взаємодії агента ІБ з ТМ наведено на рис. 2.

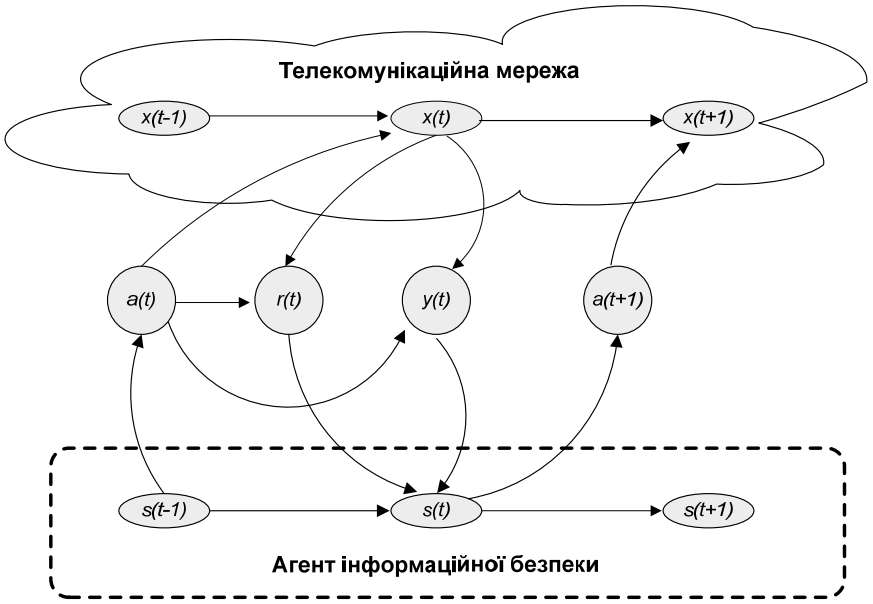

Рисунок 2 - Схема взаємодії агента з телекомунікаційною мережею

Усі часові зміни відбуваються в дискретні моменти часу. Стан ІБ ТМ описується деяким визначеним показником захищеності $x = x(t)$, що ймовірнісним чином змінюється у часі. Припустимо, що функція щільності розподілу умовної ймовірності залежить тільки від показника захищеності та дії агента в попередній момент часу:

$$\xi_{x(t)} = P\left(x(t) \mid x(t-1), a(t-1)\right), \tag{1}$$

де $x(t)$ – випадкова величина, яка описує залежність показника захищеності x від часу t;

$a(t)$ – випадкова величина, яка описує залежність дій агента a від часу t;

$\xi_{x(t)}$ – функція щільності розподілу умовної ймовірності випадкової величини $x(t)$.

Агент не може спостерігати усі компоненти стану ІБ ТМ, а спостерігає лише безпосереднє оточення. Спостережувана функція $y(t)$ описується ймовірнісною моделлю:

$$\xi_{y(t)} = P\left(y(t) \mid x(t), a(t)\right), \tag{2}$$

де $y(t)$ – випадкова величина, яка описує залежність спостережуваного показника y від часу t;

$\xi_{y(t)}$ – функція щільності розподілу умовної ймовірності випадкової величини $y(t)$.

Крім спостереження $y(t)$ агент одержує локальне заохочення $r(t)$, визначене ПІБ:

$$r(t) = E\left(x(t), a(t)\right), \tag{3}$$

де $r(t)$ – функція залежності локального заохочення r від часу t;

E – закон, який згідно з ПІБ установлює залежність локального заохочення r від x та a.

Те, що агент спостерігає, залежить від того, що він робить. Отже, враховується, що сприйняття агента є активним процесом. Сам агент має пам'ять про свій поточний стан. Новий стан $s(t)$ може змінювати за деяким законом f:

$$s(t) = f\left(s(t-1), y(t), r(t), a(t)\right), \tag{4}$$

де $s(t)$ – функція залежності поточного стану s агента від часу t;

f – закон, який визначає динаміку зміни стану s агента.

У новому стані агент виробляє керувальну дію, дотримуючись власної тактики Г:

$$a(t) = \Gamma\left(s(t)\right), \tag{5}$$

де Γ – тактика, згідно з якою агент виробляє керувальну дію a.

Метою агента є максимізація сумарного заохочення $\left(\sum_t r(t)\right) \to \max$ (тобто максимальна реалізація ПІБ) в процесі адаптації в середовищі ТМ шляхом навчання деякій оптимальній стратегії Ψ:

$$\Psi(x,a)=E\left(\sum_t \gamma^t r(t)\right)\to\max, \tag{6}$$

де Ψ – оптимальна стратегія агента, яка максимально реалізує ПІБ;

$\gamma^t r(t)$ – дисконтована функція заохочення, що гарантує кінцевість суми $\sum_t \gamma^t r(t)$ навіть у випадку, якщо агент буде адаптуватися невизначено довго.

У ТМ є виділені, досяжні з остаточною ймовірністю *термінальні* стани. Процес взаємодії агента ІБ з ТМ розбивається на окремі часові інтервали і може бути поданий мережею Петрі (рис. 3).

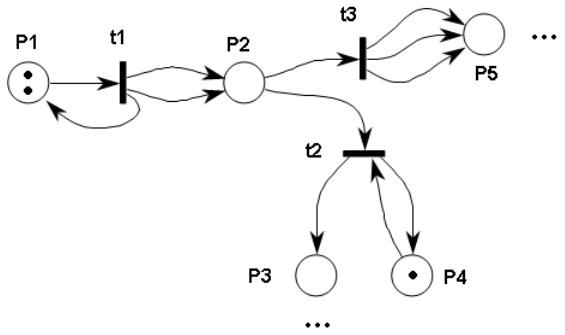

Рисунок 3 – Мережа Петрі, яка відбиває приклад процесу прийняття рішень агентом

де *P*1, *P*2, *P*3, *P*4, *P*5 – позиції мережі Петрі, що відповідають термінальним станам МС та захищеності ТМ *s (t)*; *t*1, *t*2, *t*3 – переходи мережі Петрі, що відповідають можливим рішенням *a(t)*, які може прийняти агент, дотримуючись власної стратегії.

Спираючись на розроблену ймовірнісну модель можна задати ТМ як машину кінцевих станів (Finite State Machine) або кінцевий автомат, яка є однією з базових концепцій побудови моделей сучасних технічних систем. За такого підходу МСІБ буде характеризуватися машиною, яка у будь-який момент часу перебуває в будь-якому дискретному стані. Кожному стану відповідає набір значень системних параметрів. Перехід з одного стану в інший відбувається за умови настання певної події. Машина скінченних станів може бути схарактеризована за допомогою орієнтованого графа, в якому кількість вузлів дорівнює кількості скінченних станів системи, а число ребер - усій сукупності можливих переходів з одного стану в інший. Даний підхід дозволяє виявити слабкі місця досліджуваної системи. Отже дамо ТМ у вигляді:

$$M_{\text{ТМ}}=\{S, X, Y, \partial, s(t_0)\}, \tag{7}$$

де $S = \{ s(t) \}$ – множина внутрішніх станів системи;

$X = \{ x(t) \}$ – множина вхідних сигналів;

$Y=\{ y(t) \}$ – множина вихідних сигналів;

∂ – функція переходів;

$s(t_0)$ – початковий стан системи.

Припустимо, що є відомі множина дозволених (безпечних) станів $S_{\text{Б}}$ і множина заборонених (небезпечних) станів $S_{\text{НБ}}$ системи, а також множини безпечних вихідних сигналів $Y_{\text{Б}}$ і небезпечних вихідних сигналів $Y_{\text{НБ}}$:

$$S=S_{\text{Б}}\cup S_{\text{НБ}}, \qquad Y=Y_{\text{Б}}\cup Y_{\text{НБ}}. \tag{8}$$

Надалі будемо вважати, що безпечний стан ТМ у момент t – це перебування її в безпечному стані $s(t) \in S_{\text{Б}}$ і наявність безпечного для даного стану вхідного сигналу $y(t) \in Y_{\text{Б}}$. Отже, перехід у заборонений стан $s^* \in S_{\text{НБ}}$ і поява небезпечного сигналу на виході задаються початковим станом $s(t_0)$ і значенням, послідовністю або комбінацією вхідних сигналів, які задають послідовність переходів, що приводить до забороненого стану. Таким чином, завдання збереження захищеності полягає в контролі поточного стану системи й відсутності можливості переходу в заборонений стан. Мета діяльності агента полягає в перевірці зазначених властивостей. Отже, агент виконує оцінку можливості та контроль переходу системи в момент t з безпечного стану в небезпечний на основі інформації про вхідні й вихідних дані системи на кінцевому інтервалі часу [0, t].

Внутрішній стан ТМ не є повністю доступним для спостереження, тому припустимо, що аналіз поточного стану ТМ можливий тільки за її вихідними значеннями. Таким чином, ТМ можна

подати у вигляді дискретної системи замкненого типу з негативним зворотним зв'язком. Модель являє собою «чорний ящик», що перебуває в деякий момент t у стані $s(t)$, при цьому його вихідний сигнал – $y(t)$, а на вхід надходить сигнал $x(t)$. Мультиагентна система порівнює вихідний сигнал ТМ з профілем фільтрації (ПФ) МЕ. Помилка подається потім на засоби керування $a(t)$, які реалізують негативний зворотний зв'язок.

Мультиагентну систему також можна задати у вигляді машини скінченних станів:

$$M_{\text{МС}} = \{\underline{S}, \underline{X}, \underline{Y}, \underline{\partial}, \underline{s(t_0)}\}, \tag{9}$$

де $\underline{S}=\{\underline{s(t)}\}$ – множина внутрішніх станів мультиагентної системи;

$\underline{X}=\{\underline{x(t)}\}$ – множина вхідних сигналів (вихідних сигналів $M_{\text{ТМ}}$);

$\underline{Y}=\{\underline{y(t)}\}$ – множина вихідних сигналів;

$\underline{\partial}$ – функція переходів;

$\underline{s(t_0)}$ – початковий стан мультиагентної системи.

При цьому, вихідні сигнали $M_{\text{ТМ}}$ є вхідними сигналами $M_{\text{МС}}$, тобто $\underline{X} = Y$, а кількість станів мультиагентної системи буде меншою за кількість станів ТМ, тобто $card\ \underline{S} \le card\ S$. Збільшення кількості станів мультиагентної системи буде означати більш точне подання ПФ у ПІБ ТМ. Однак це може привести до надмірного ускладнення мультиагентної системи. Крім того, зі зростанням складності мультиагентної системи через можливі збої виникає завдання її верифікації.

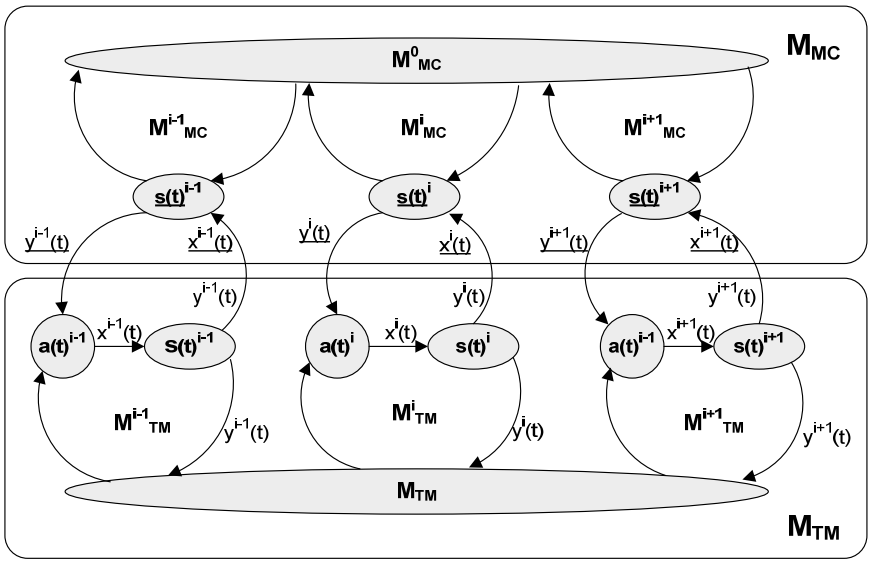

Рисунок 4 – Граф машини скінченних станів мультиагентної системи інформаційної безпеки

ТМ є розподіленою системою, її можна представити у вигляді сукупності вузлів окремих МЕ, $M_{\text{ТМ}} = \{M^i_{\text{ТМ}}\}$. Отже, поняття захищеності застосовне й до ТМ у цілому, і до кожного вузла окремо. У цьому випадку є автономний елемент (агент) $M^i_{\text{МС}}$ для кожного вузла мережі $M^i_{\text{ТМ}}$. Також існує центральний агент системи $M^0_{\text{МС}}$. Сукупність таких агентів $M_{\text{МС}} = \{M^i_{\text{МС}}\}$, $i = 0, \ldots, l$ утворить мультиагентну систему (рис. 4).

Підсумуємо отримані в даній роботі результати. Запропонована схема мультиагентної системи керування міжмережними екранами. Розроблено ймовірнісну модель взаємодії агента ІБ з телекомунікаційною мережею. На основі цієї моделі побудована мережа Петрі, яка відбиває приклад процесу прийняття рішень агентом, а також граф та машину скінченних станів мультиагентної системи інформаційної безпеки в телекомунікаційній мережі.

Результати дослідження свідчать, що в цілому мультиагентні системи є адекватним, актуальним відбиттям та засобом реалізації політики інформаційної безпеки, що динамічно змінюється під впливом змін в телекомунікаційній мережі, з появою нових ризиків і загроз. Напрямом подальших досліджень є уточнення, деталізація та конкретизація параметрів розроблених математичних моделей.

Література

1. *Павлов И.Н., Полознюк А.Н.* Анализ моделей защиты информации // Зв'язок. – К.. – №1. – 2006.
2. *Гладыш С.В.* Использование нечетких сетей Петри для построения модели распределения ресурсов информационной безопасности информационно-телекоммуникационных сетей // Вісник Державного університету інформаційно-комунікаційних технологій. – №1, 2007.
3. *Гладыш С.В.* Настройка параметров модели распределения ресурсов информационной безопасности с помощью нечетких нейронных сетей // Вісник Севастопільского національного технічного університету. Серія «Інформатика, електроніка, зв'язок». – №1, 2007
4. *Гладыш С.В.* Модель распределения ресурсов информационной безопасности в телекоммуникационных системах на базе нейро-фаззи сети Петри // Інформаційні технології та комп'ютерна інженерія. – №1, 2007.
5. *Терехов С.А.* Нейро-динамическое программирование автономных агентов. Лекции по нейродинамическому программированию. – М.: МИФИ, 2004. – 20 с.
6. *Тимофеев. А.В.* Мультиагентное и интеллектуальное управление сложными робототехническими системами // Юбилейный сборник "Теоретические основы и прикладные задачи интеллектуальных информационных технологий", посвящённый 275-летию РАН и 20-летию СПИИ РАН-СПб. – СПИИ РАН, 1999. – С. 71-81.
7. *Валеев С.С., Бакиров Т.К., Камалетдинов Т.Р.* Многоагентная система анализа защищенности вычислительных сетей // Известия ТРТУ. – 2003. – Тематический выпуск «Информационная безопасность». – С.242–243.
8. *Carvalho M., Cowin T., Suri N., Breedy M., Ford K.* Using Mobile Agents as Roaming Security Guards to Test and Improve Security of Hosts and Networks. // Proceedings of the 2004 ACM Symposium on Applied Computing (SAC'04). – ACM, 2004.
9. *Грушо А.А., Тимохина Е.Е.* Распределенные атаки на распределенные системы // Jet Info. – 2006. - №1.
10. *Pedireddy T., Vidal J.* A Prototype Multi Agent Network Security System. // Proceedings of the AAMAS'03. – ACM, 2003.
11. *Menezes R.* Self-Organization and Computer Security. // Proceedings of the 2005 ACM Symposium on Applied Computing (SAC'05). – ACM, 2005.
12. *Котенко И. В.* Многоагентные модели противоборства злоумышленников и систем защиты в сети Интернет // Третья Общероссийская Конференция «Математика и безопасность информационных технологий» (МаБИТ-04). - М: МГУ, 2004.
13. *Michael J. Wenstrom.* Managing Cisco Network Security. – Indianapolis, USA: Cisco Press, 2001. – 768 p.