ОБҐРУНТУВАННЯ СТРУКТУРИ ЕКСТРЕМАЛЬНОГО РЕГУЛЯТОРА ПО ПРОДУКТИВНОСТІ АВТОМАТИЗОВАНОГО ПРОЦЕСУ ЕЛЕКТРОЕРОЗІЙНОЇ ОБРОБКИ

У даній статті обґрунтовується функціональна схема екстремального регулятора по продуктивності процесу розмірної обробки дугою, що синтезована на основі аналізу технологічного процесу і реалізації його параметрів, які мають стохастичний характер. Запропонований алгоритм роботи регулятора з використанням кореляційного аналізу вибірок випадкового процесу.

Ключові слова: екстремальний регулятор, розмірна обробка дугою.

Савеленко Григорий Владимирович, *ассистент, кафедра экономики и организации производства, Кировоградский национальный технический университет, Украина,* ***e-mail: savelenko@mail.ru****.*

Ермолаев Юрий Алексеевич, *кандидат технических наук, доцент, кафедра автоматизации производственных процессов, Кировоградский национальный технический университет, Украина,* ***e-mail: ermolaevua@ukr.net****.*

Савеленко Григорій Володимирович, *асистент, кафедра економіки та організації виробництва, Кіровоградський національний технічний університет, Україна.*

Єрмолаєв Юрій Олексійович, *кандидат технічних наук, доцент, кафедра автоматизації виробничих процесів, Кіровоградський національний технічний університет, Україна.*

Savelenko Gregory, *Kirovograd National Technical University, Ukraine,* ***e-mail: savelenko@mail.ru****.*

Yermolaev Yury, *Kirovograd National Technical University, Ukraine,* ***e-mail: ermolaevua@ukr.net***

УДК 004.056, 5.621.396
DOI: 10.15587/2312-8372.2014.32792

Хлапонін Ю. І.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

Представлено аналіз розвитку інформаційно-телекомунікаційних мереж нового покоління. Метою проведених досліджень була розробка наукових основ ситуаційного управління безпекою в ІТМ на основі інтелектуальних технологій. Наведена узагальнена структура системи інтелектуального управління безпекою. Представлено структуру нейросистеми оцінки рівня безпеки в ІТМ та описано принцип її функціонування.

Ключові слова: *інформаційно-телекомунікаційна мережа, інтелектуальні технології, загрози, нейросистема.*

1. Вступ

Розвиток інформаційних послуг вимагає рішення завдань ефективного управління інформаційними ресурсами з одночасним розширенням функціональності інформаційно-телекомунікаційних мереж (ІТМ). У 90-х роках минулого сторіччя передбачалося, що ідея створення ІТМ буде втілена за допомогою концепції інтелектуальної мережі. У 1993 році Міжнародний союз електрозв'язку (ITU-T) затвердив перші специфікації технології Intelligent Network (IN). Основним принципом побудови інтелектуальної мережі стало логічне розділення рівня комутації та надання послуг, завдяки чому з'явилася можливість створювати нові телекомунікаційні послуги [1].

В 2014 році світовий лідер у сфері інформаційно-телекомунікаційних технологій компанія Huawei, повідомила про розвиток нового покоління бездротових мереж 5G. Технології 5G підтримуватимуть 1000-разове збільшення потужності, підключення мінімум 100 мільярдів пристроїв, а також 10 Гб/с індивідуальної активності користувача. Очікується, що 5G-технології активно розвиватимуться в наступному десятиріччі [2].

Одночасно з розвитком технологій постає питання безпеки в інформаційно-телекомунікаційних мережах (ІТМ). З точки зору забезпечення безпеки найбільш важливими властивостями мереж є: конфіденційність (використання інфраструктури або її частини); цілісність (інфраструктури); доступність (служб та сервісів); спостереженість (за використанням інфраструктури або її частини); прихованість (використання та управління інфраструктурою) [3].

Якщо для захисту інформації найбільш важливими заходами є запобігання загрозам конфіденційності та цілісності, то в (ІТМ) основні зусилля повинні бути направлені на запобігання загрозам доступності служб (в ІТМ атаки з метою порушення доступності реалізуються простіше) та спостереженість за використанням інфраструктури (або її частини). Доступ до інформації відбувається шляхом формування та обробки запитів до відповідних служб, які функціонують на різних серверах. Тому, в ІТМ розглядається саме доступність відповідних служб.

Таким чином можна зробити висновок, що безпека в ІТМ має істотні відмінності від забезпечення безпеки конкретної інформації в будь-якій визначеній системі. Це потребує застосування нових підходів по створенню систем безпеки в ІТМ, в тому числі, з використанням інтелектуальних технологій.

Цим обґрунтовується актуальність проведення даних досліджень.

2. Аналіз літературних даних і постановка проблеми

Аналіз функціонування ІТМ мереж показав, що на даному етапі розвитку мереж забезпечити їх ефективну роботу та, відповідно, безпеку досить проблематично, а враховуючи складність структури, її багатовимірність та багаторівневу будову, вкрай незручно. Для вирішення цієї наукової проблеми пропонується застосування інтелектуальних технологій. Шляхи вирішення даної проблеми опубліковані в роботах [4–6].

На сьогоднішній день інтелектуальним технологіям приділяється велика увага [7, 8]. Інтелектуальні системи останнім часом стали досить розповсюдженим комерційним продуктом, що знаходить широкий попит користувачів-фахівців у найрізноманітніших областях інженерно-технічної й науково-технічної сфер діяльності.

Створення систем безпеки в ІТМ, які орієнтуються для роботи в умовах неповноти або нечіткості вихідної інформації, невизначеності зовнішніх впливів та середовища функціонування, вимагає залучення нетрадиційних підходів до управління безпекою в ІТМ з використанням методів і технологій штучного інтелекту. Такі системи, названі інтелектуальними системами безпеки, утворять зовсім новий клас, для якого не тільки принципи побудови, методи аналізу й синтезу перебувають у стадії розвитку, але й основні поняття й визначення мають потребу в ретельному методичному проробленні.

Очевидно, що при наявності різного роду невизначеностей високий рівень автономності, адаптивності й надійності систем управління безпекою повинен забезпечуватися за рахунок підвищення їхніх інтелектуальних можливостей, заснованих на обробці спеціальних знань. Становлення концепції інтелектуальних систем управління безпекою обумовлює цілий ряд принципових питань. Перше з них пов'язане із чітким визначенням знань, не тільки як форми машинного подання інформації, але і як інструмента для організації принципів управління безпекою. При цьому найважливішим аспектом є аналіз можливостей і особливостей застосування тих або інших інформаційних технологій для обробки знань у завданнях інтелектуального управління [8].

Метою проведених досліджень була розробка наукових основ ситуаційного управління безпекою в ІТМ на основі інтелектуальних технологій.

Для досягнення поставленої мети необхідно:

1. Застосувати теорію нечітких продукційних моделей (мереж), які по своїй структурі ідентичні багатошаровим нейронним мережам.
2. Обґрунтувати можливість застосування нейроінформаційних технологій при рішенні задач адаптивного управління інформаційною безпекою.

3. Результати досліджень системи управління безпекою в ІТМ на основі інтелектуальних технологій

Виходячи з ключових положень теорії ситуаційного управління кожному класу загроз (рис. 1), виникнення яких вважається припустимим у процесі функціонування мережі, ставитися у відповідність деяке рішення по управлінню та протидії таким загрозам.

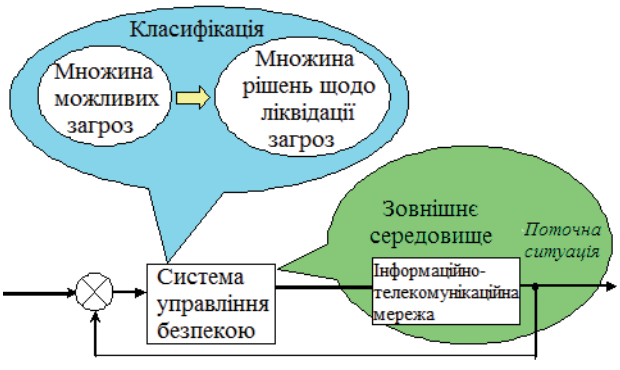

Рис. 1. Принцип ситуаційного управління інформаційною безпекою

Тоді сформована ситуація, обумовлена поточним станом як самої мережі, так і її зовнішнього середовища й яка ідентифікується за допомогою вимірювально-інформаційних засобів системи безпеки, може бути віднесена до деякого класу, для якого необхідне управління вже вважається відомим.

Таким чином, практична реалізація концепції ситуаційного управління безпекою на основі сучасних інтелектуальних технологій припускає наявність розгорнутої бази знань про принципи побудови й мету функціонування системи, специфіку використання різних алгоритмів, особливості виконавчих сегментів та мережі в цілому, а також про існуючі та той момент можливі типи загроз для інформації (DDos-атаки, віруси, «трояни» тощо). Важливо відзначити, що головна архітектурна особливість, що відрізняє інтелектуальну систему управління безпекою (рис. 2) від побудованої по «традиційній» схемі, пов'язана з підключенням механізмів зберігання й обробки знань для реалізації здатностей по виконанню необхідних функцій у неповно заданих (або невизначених) умовах при випадковому характері зовнішніх впливів. До впливів подібного роду можуть відноситися непередбачена зміна цілей, експлуатаційних характеристик ІТМ й об'єкта управління, параметрів зовнішнього середовища, поява нових видів загроз й т. ін. Крім того, склад системи при необхідності доповнюється засобами самонавчання, що забезпечують узагальнення досвіду, що накопичується, і на цій основі поповнення знань.

Практичне втілення цієї концепції припускає вибіркове використання тих або інших технологій обробки знань залежно від специфіки завдань, що розв'язуються, особливостей керованого об'єкта, його функціонального призначення, умов експлуатації. Як показує огляд численних робіт з розвитку методів обробки знань, одна з передових тенденцій у цій області пов'язана зі спробами інтеграції різних інтелектуальних технологій для об'єднання їхніх переваг. Так, наприклад, одночасне забезпечення високої функціональної гнучкості й швидкодії може досягатися за рахунок комплексного застосування технологій експертних систем і нейромережевих структур.

Висока ефективність нейроінформаційних технологій при рішенні задач адаптивного управління інформаційною безпекою вже найближчим часом може зробити їх незамінними при створенні нових поколінь систем захисту. Актуальність досліджень штучних нейронних мереж підтверджується різноманіттям їх можливого застосування.

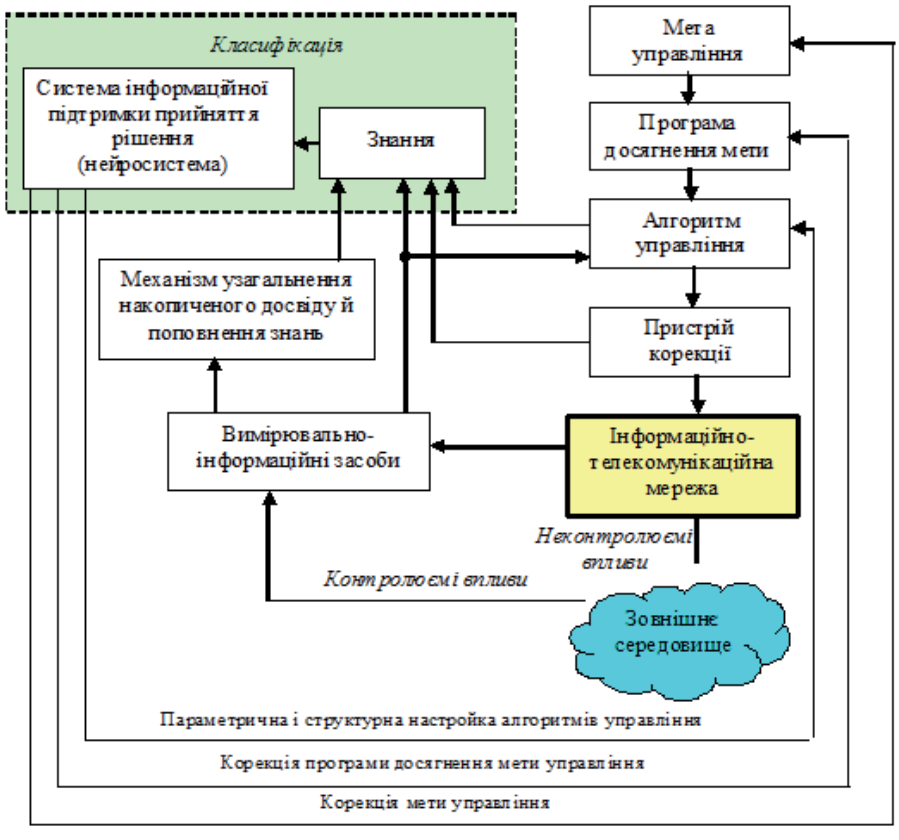

Рис. 2. Узагальнена структура системи інтелектуального управління безпекою

Число нейроподібних елементів (нейронів) у шарі, визначається обсягом статистичної вибірки. При цьому великі статистичні вибірки збільшують розмірність простору станів захищеності, представлених технологічним портретом захищеності (набором симптомів), а малі не дозволяють однозначно зв'язати симптоми з діагнозом. Оптимальним буде портрет захищеності, що дозволяє одержати необхідний обсяг інформації щодо захищеності ІТМ від певного набору загроз в певний час. При цьому обсяг статистичної вибірки буде визначатися кількістю застосованих систем виявлення загроз (антивіруси, системи виявлення атак, мережеві екрани тощо). Сукупність нейронних ансамблів (шарів) являє собою нейронну мережу (НМ). Такі НМ є спрощеною марковською моделлю. Однак вони мають асоціативні властивості, що нагадують властивості біологічних систем [10].

Оскільки всі штучні нейроні мережі базуються на концепції нейронів, з'єднань та передатних функцій, існує подібність між різними структурами або архітектурами нейронних мереж. Більшість змін походить з різних правил навчання [9].

Структура нейросистеми (НС) оцінки рівня безпеки в ІТМ, яка представлена на рис. 3 включає m-нейронних ансамблів (шарів), які визначаються кількістю класів станів захищеності інформації від певного виду загроз. Клас станів захищеності відповідає нейронному шару, а число класів визначається глибиною пошуку загрози, тобто структурним елементом, що призначений для виявлення певного класу загроз безпеці в ІТМ, а число класів визначається параметрами, які виявляються вимірювально-інформаційними засобами системи безпеки з метою визначення стану захищеності інформації в ІТМ.

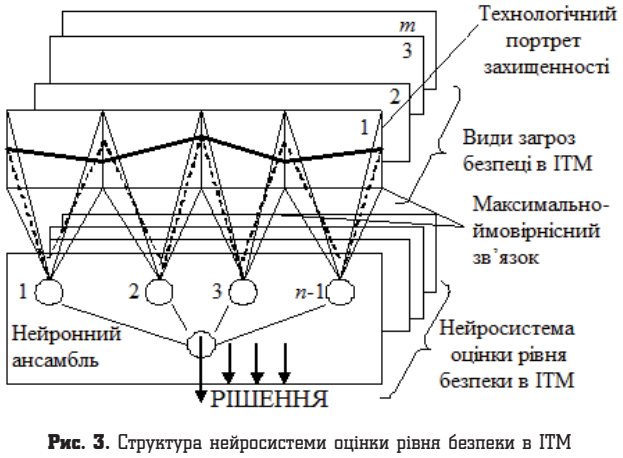

Рис. 3. Структура нейросистеми оцінки рівня безпеки в ІТМ

4. Висновки

1. Доведено, що безпека в ІТМ має істотні відмінності від забезпечення безпеки конкретної інформації в будь-якій визначеній системі.
2. Наведена структура системи інтелектуального управління безпекою в ІТМ.
3. Наведена структура нейросистеми оцінки рівня безпеки в ІТМ.
4. Вперше введено поняття технологічних портретів захищеності як сукупності станів захищеності, які відповідають виявленим загрозам в ІТМ в певний момент часу.

Література

1. Pinnes, E. L. Operations and Management for Next Generation Network [Electronic resource] / E. L. Pinnes // 2000 Asia-Pacific Network Operations and Management Symposium «New Management Paradigms and Technologies Towards the Internet Millennium», 11–13 October 2000, Nara-Ken New Public Hall, Nara, Japan. — Available at: \www/URL: http://www.ieice.or.jp/cs/tm/apnoms/2000/tutorial.htm. — 15.11.2014.
2. Нове покоління бездротових мереж 5G! [Електронний ресурс]. — Режим доступу: \www/URL: http://consumer.huawei.com/ua/news/show_one/27. — 31.01.2014.
3. Хлапонін, Ю. І. Загальні характеристики загроз в кіберпросторі [Текст]: тези доп. / Ю. І. Хлапонін, В. В. Овсянніков, Н. А. Паламарчук // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: VI наук.-практ. сем. Військового інституту телекомунікацій та інформатизації НТУУ «КПІ», 20 жовтня 2011 р. — К., 2011. — С. 157.
4. Артеменко, М. Ю. Нейронні мережі та їх застосування в телекомунікаційних системах [Текст] / М. Ю. Артеменко, Л. Н. Беркман, С. В. Толюпа // Радіотехніка. — 2007. — Вип. 134. — С. 45–53.

5. Бакланов, И. Г. NGN: принципы построения и организации [Текст] / И. Г. Бакланов. — М.: Эко-Трендз, 2008. — 468 с.
6. Герасимов, Б. М. Человеко-машинные системы принятия решений с элементами искусственного интеллекта [Текст] / Б. М. Герасимов, В. А. Тарасов, И. В. Токарев. — К.: Наукова думка, 1993. — 168 с.
7. Макаров, И. М. Интеллектуальные системы автоматического управления [Текст] / И. М. Макаров. — М.: Физматпит, 2005. — 573 с.
8. Поспелов, Д. А. Искусственный интеллект в зарубежных исследованиях [Текст] / Д. А. Поспелов, В. П. Стефанюк // Информационные материалы. Кибернетика. — М.: Информприбор, 1986. — № 3. — С. 3–25.
9. А. с. 1663661 СССР. Устройство для обучения распознаванию образов [Текст] / Хлапонин Ю. І., Корнейчук Н. П., Зарицкий А. Ф., Брынцев А. П. (СССР). — 4944920/24, заявл. 18.11.90; опубл. 16.05.91. — 2 с.
10. Клейнрок, Л. Теория массового обслуживания [Текст] / Л. Клейнрок. — М.: Машиностроение, 1979. — 342 с.

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

Представлен анализ развития информационно-телекоммуникационных сетей нового поколения. Целью проведенных исследований была разработка научных основ ситуационного управления безопасностью в ИТМ на основе интеллектуальных технологий. Приведена обобщенная структура системы интеллектуального управления безопасностью. Представлена структура нейросистемы оценки уровня безопасности в ИТС и описан принцип ее функционирования.

Ключевые слова: информационно-телекоммуникационная сеть, интеллектуальные технологии, угрозы, нейросистема.

Хлапонін Юрій Іванович, *кандидат технічних наук, старший науковий співробітник, доцент, кафедра засобів захисту інформації, Національний авіаційний університет, Київ, Україна,* ***e-mail: yfcnz0408@ukr.net****.*

Хлапонин Юрий Иванович, *кандидат технических наук, старший научный сотрудник, доцент, кафедра средств защиты информации, Национальный авиационный университет, Киев, Украина.*

Khlaponin Yuriy, *National Aviation University, Kyiv, Ukraine,* ***e-mail: yfcnz0408@ukr.net***