УДК 004.8

Костюк Ю.В., старший викладач
Степашкіна К.В., асистент
Державний торговельно-економічний університет, м. Київ, kostyuk.yu@ukr.net

МОДЕЛЮВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

На сучасному етапі розвитку інформаційно-комунікаційних систем здійснюється їх інтеграція в єдині системи і, зокрема, продовжується інтенсивний розвиток єдиної інформаційно-телекомунікаційної системи як науково-технічної та функціональної бази для реалізації концепції інформатизації, одна із стратегій якої полягає у створенні єдиного інформаційного простору. Більшість автоматизованих систем обробки інформації, в тому числі і автоматизовані інформаційні системи, і єдині автоматизовані інформаційні системи, і підсистеми комплексної автоматизованої інтелектуальної системи характеризуються інформаційною розподіленістю, семантичною доступністю для інформаційного впливу, різним рівнем складності структурної організації. Вони визначають безліч технологічних процесів обробки інформації, безліч подій та станів, які не завжди можуть бути чітко формалізовані, виразно та повно описані у вигляді семантичних правил реагування. Це створює передумови загострення інформаційного протистояння на якісному новому рівні. У зв'язку з цим забезпечення інформаційної безпеки (ІБ) на рівні взаємодії інформаційно-комунікаційних систем, їх хостів та мережевої інфраструктури є одним із важливих завдань при оптимальному розподілі ефективного функціонування систем захисту.

Для успішного використання сучасних інформаційних технологій необхідно ефективно керувати не лише мережею, а й системою захисту інформації (СЗІ), при цьому на рівні сегмента інформаційно-телекомунікаційної системи має працювати система, здатна оптимізувати захищеність інформаційно-комунікаційного середовища сегмента підприємства та мінімізувати загальну шкоду при порушеннях ІБ. Для цього буде потрібно створення систем та моделей управління подіями інформаційної безпеки, спрямованих на ідентифікацію загроз, активацію необхідних механізмів захисту, які враховують структуру створюваної СЗІ певної інформаційно-комунікаційної системи підприємства, здатної до навчання та адаптації в нечітких умовах функціонування [1, 2].

Важливим чинником є розробка та вдосконалення моделей управління захистом інформації у сегменті інформаційно-комунікаційної системи підприємства для вирішення задачі забезпечення необхідного рівня інформаційної безпеки протягом життєвого циклу системи захисту інформації в умовах невизначених шкідливих дій з використанням інтелектуальної підтримки прийняття рішень. Для вирішення проблеми необхідно: проаналізувати існуючі сучасні системи управління захистом інформації та особливості їх застосування під час реалізації єдиної системи інформаційної безпеки в умовах інформатизації; розробити моделі загроз інформаційній безпеці для побудови систем управління захистом інформації у сегменті інформаційно-комунікаційної системи підприємства, що забезпечує ефективне оперативне управління за умов невизначеності стану інформаційного середовища; розробити алгоритм оцінки рівня захищеності інформаційно-комунікаційної системи та ефективності системи управління захистом інформації у сегменті інформаційно-комунікаційної системи підприємства; розробити модель та алгоритм функціонування адаптивної інтелектуальної системи управління захистом інформації на основі нейро-нечіткої побудови мереж, теорії нечіткої логіки та множин. Алгоритм функціонування моделі, що відрізняється блоковою структурою адаптивної системи захисту інформації комплексної автоматизованої інтелектуальної системи демонструє етапи навчання нечітких нейронних та нейро-нечітких мереж для класифікації необхідних механізмів захисту та ідентифікації невідомих загроз [2].

Отже, нечіткі нейронні мережі можна розглядати як елементи моделі інтелектуальної системи управління захистом інформації. В ієрархічній побудові структури інтелектуальної моделі системи управління захистом інформації інформаційно-телекомунікаційної системи, заснованої на нейронечітких мережах, інтелектуальні інформаційні системи та системи інтелектуального управління використовують з метою вдосконалення інформаційних технологій для забезпечення антитерористичної та протикримінальної захищеності [3]. Структурно-функціональну схема алгоритму формування моделі адаптивної інтелектуальної системи захисту інформації та її покрокове виконання, використовуючи як нечіткі посилки вектори вхідних ознак атак внизу ієрархії СЗІ, реалізовують механізм побудови системи нечітких продукційних правил для ідентифікації загроз. На верхньому рівні ієрархії захисту для кожного рівня багаторівневої СЗІ вирішується задача класифікації механізмів захисту (нечіткі висновки) по вектору нечітких ознак загроз, для нейтралізації наслідків яких механізми захисту призначені (механізм системного знищення програм, механізм блокування доступу до ресурсу, механізм зниження пріоритету користувача, механізм ідентифікації та аутентифікації тощо) певного рівня багаторівневої СЗІ [2, 3].

Активний розвиток інформатизації та обумовлене цим процесом значне зростання відомчих інформаційних активів підприємства, у тому числі конфіденційного характеру, вимагає ухвалення адекватних та своєчасних рішень щодо нарощування потенціалу системи захисту інформації в галузі протидії загрозам інформаційної безпеки, що зростають у міру інтенсифікації розвитку інформаційних технологій [4]. Актуалізація заходів на адміністративному рівні забезпечення інформаційної безпеки, складається з таких заходів: організація комплексу заходів щодо захисту від комп'ютерних атак на критично важливі сегменти інформаційної інфраструктури підприємства; розробка комплексу заходів щодо забезпечення інформаційної безпеки та захисту даних інформаційних систем з урахуванням «хмарної архітектури»; застосування ефективних механізмів захисту від несанкціонованого доступу під час створення повномасштабної системи доступу різних категорій користувачів системи до інформаційних активів, включаючи впровадження у діяльність системи мобільного захищеного віддаленого доступу до інформаційних ресурсів; розробка програмно-технічного рішення щодо забезпечення комплексного захисту інформації [3, 4].

Все це дозволяє реалізувати новий рівень розвитку системи інформаційної безпеки підприємства, перейти на сучасний етап функціонування єдиної системи інформаційної безпеки інформаційно-комунікаційних систем підприємства та створити надійну адаптивну систему, здатну до навчання при різних інформаційних впливах, що мають ознаки шкідливих атак, які найчастіше досить складно формалізувати, чітко і однозначно математично описати. Алгоритмічні схеми, структура та моделі побудови адаптивної системи управління захистом інформації в інформаційно-телекомунікаційній системі, а також математичний апарат нейро-нечіткого опису у вигляді правил продукції, які адекватно відображають отримані результати та дозволяють створити ефективну модель управління подіями інформаційної безпеки однієї з інформаційно-комунікаційних систем підприємства.

Список посилань

1. Технології захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]: навчальний посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 213 с.

2. Бурячок, В. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно–телекомунікаційних систем / В. Л. Бурячок // Захист інформації. НАУ. - К. –2011. – №3. – с. 1-9.

3. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко. – К.: ДУТ, 2015. – 345 с.

4. Соколов В.Ю. Інформаційні системи і технології: навч. посіб. / В.Ю. Соколов. – К.: ДУІКТ, 2010. – 138 с.