

ЗАСТОСУВАННЯ НЕЙРОМЕРЕЖ ДЛЯ АНАЛІЗУ ЗАГРОЗ В ІТС

При створенні і в ході експлуатації ІТС неминує постає питання про її захист. Виявлення вразливих місць в системі і додатках стає першим кроком в досягненні необхідного рівня захисту. Рішення даної задачі покладається на адміністратора безпеки комп'ютерної мережі. Для рішення задачі пошуку уразливостей адміністратором використовуються засоби аналізу захищеності, яким притаманні недоліки, що призводить до зниження ефективності контролю захищеності комп'ютерної мережі. Крім того, адміністратор змушений витратити час на ручні операції, пов'язані з підготовкою контролю захищеності та інформаційного підготовкою прийняття рішення і усунення виявлених уразливостей.

У зв'язку з цим доцільне використання постійного контролю захищеності комп'ютерної мережі в автоматичному режимі. При цьому виникає необхідність створення нових засобів аналізу захищеності.

Для вирішення даних задач можливе застосування нейромережевих методів оцінки рівня захищеності інформації.

Функціонування нейронної мережі (НМ) полягає в перетворенні вхідної технологічної інформації про стан захищеності у певну сукупність вихідних сигналів. Перетворення відбувається за рахунок зміни внутрішнього стану НМ. Нейрони, з яких складається НМ, представляють собою прості процесори, які налаштовані на реагування на певні види загроз, такі як спроба несанкціонованого доступу до корпоративної мережі, спроба модифікації програмного забезпечення, віруси, атаки типу „відмова в обслуговуванні” тощо. Необхідним є визначення правила активації НМ, яке дозволяє визначити вихідний сигнал по сукупності вхідних.

У цій конфігурації нейромережа отримує весь трафік і аналізує інформацію на наявність негативних впливів з боку порушника.

Структура нейромережевої системи оцінки рівня захищеності інформації включає m-нейронних ансамблів (шарів), які визначаються кількістю процесорів, які налаштовані на реагування певному виду загроз. Стан захищеності відповідає нейронному шару, а число класів визначається параметрами, які обираються заздалегідь, в залежності від кількості видів загроз, які може виявляти. З появою нових загроз НМ „навчається” і додає до свого арсеналу реагування на загрози новий клас.

У зв'язку з обмеженими можливостями існуючих систем виникає перспектива розробки адаптивних систем аналізу даних і управління засобами захисту. Системи аналізу загроз в інформаційно-телекомунікаційних системах на базі нейронних мереж в перспективі могли б вирішити багато проблем, що не вирішуються існуючими системами.

Науковий керівник – к.т.н., с.н.с., доц., Ю.І. Хлапонін