

ВИЯВЛЕННЯ ЗОНДУВАННЯ АТАКИ З ВИКОРИСТАННЯМ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

За умови стрімких темпів розвитку інформаційних технологій, збільшення кількості загроз інформації, ступеня невизначеності їх виникнення і реалізації, а також складності систем захисту інформації та їх спеціалізованої спрямованості, набуває актуальності завдання отримання узагальненої оцінки рівня захищеності інформації на основі методології, що враховує як кількісні, так і якісні показники оцінки. На сьогоднішній день, практично на будь-якому об'єкті ОІД реалізована комп'ютерна мережа. У зв'язку з швидким поширенням комп'ютерних мереж, з'явилося багато проблем з безпекою.

В останні роки число нападів на мережу різко збільшилося, тому забезпечення безпеки мережних ресурсів є дуже істотним завданням. Ці напади є основами інших атак типу DOS, R2U, U2R та ін. Отже, системи захисту від таких атак - це необхідність. Ці атаки не втягуються в активну діяльність, але в основному знаходяться в пасивному стані, і з'ясовують, які машини активні або перебувають у мережі, які сервіси використовуються користувачем і т. д. Насправді зловмисники або хакери використовують різні зондувальні інструменти, щоб отримати недоліки у системі, різного роду установки або алгоритми, які можуть допомогти в їх активних атаках. У процесі виявлення вторгнень є дві категорії - зловживання і виявлення аномалій. Категорія зловживання - це загальна категорія виявлення вторгнень, яка працює шляхом визначення видів діяльності, які змінюються в залежності від встановлених закономірностей для користувачів або груп користувачів. Це, як правило, передбачає створення баз знань, у яких міститься характеристика досліджених видів діяльності. Другий метод передбачає порівняння діяльності користувача з відомою поведінкою зловмисників, що намагаються проникнути в систему. Виявлення зловживань також використовує базу знань інформації. В основному, засоби виявлення атак використовують оцінки параметрів, таких як позитивні і хибно-негативні рівні виявлення. Помилкове спрацювання відбувається, коли система класифікує дії як аномальні (можливого зараження), коли це законні дії. У той час як хибно-негативні виникають, коли фактичні нав'язливі дії мали місце, але система дозволяє їм передати інформацію в якості природної поведінки.

Основна проблема захисту інформації шляхом створення штучної нейронної мережі є велика кількість хибно-позитивних і хибно-негативних спрацювань. Для виявлення кількісних характеристик були по чергово введені в мережу різного роду пробники атак.

Результатом є те, що наша система є найбільш ефективною для захисту інформації, та мають майже 100% захищеність та близько до 0% хибно-позитивних і хибно-негативних спрацювань.