УДК 004.021
Чемерис К.М.[1], Дейнега Л.Ю.[2]
[1]студент гр. КНТ-137 НУ «Запорізька політехніка»
[2]старш. викл. НУ «Запорізька політехніка»

ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ДІЙ І АТАК В МЕРЕЖАХ МЕТОДОМ ВЕЙВЛЕТ-АНАЛІЗУ

В даний час Інтернет є місцем високої ділової активності. Тому в даний час особливо актуальні проблеми, що стосуються виявлення мережних атак і аномалій мережевого трафіку з метою попередження подальшого вторгнення і зниження ризиків від подібних порушень. Далі представлено аналіз існуючих основних методів вирішення задачі виявлення мережних атак, вибір методів та їх застосування для виявлення вторгнень.

Мережні аномалії можна поділити на дві основні групи: програмно-апаратні відхилення і проблеми безпеки. До програмно-апаратних відхилень належать: апаратні несправності, помилки конфігурації, помилки програмного забезпечення та проблеми продуктивності обладнання. Порушення мережевої безпеки містять: сканування, атаки з метою відмови від обслуговування, вірусну активність, поширення програмних "черв'яків", експлуатацію вразливостей, аналізатори трафіку і мережні модифікатори. Найбільший економічний збиток операторам зв'язку наносять атаки з метою перевантаження мереж або сервісів і мережна вірусна активність.

Мережна атака - деякий набір дій (активність), що має на меті зробити з комп'ютером (сервером) якісь дії віддалено. Дії, зазвичай, є небажаними, і дуже важливо вчасно застосовувати алгоритми виявлення мережних атак.

Застосування алгоритму на основі вейвлет-перетворення є однією з найбільш перспективних технологій пошуку потрібної інформації в базах даних мережної безпеки. Вейвлет - це математична функція, яка дозволяє аналізувати різні частотні компоненти даних [1]. Оскільки вейвлети мають хорошу частотно-часову адаптацію, вони можуть служити зручним інструментом для дослідження частотних характеристик нестаціонарного сигналу. Перевага такого підходу - характерні деталі, які можуть залишатися непоміченими при одному масштабі, легко можуть бути виявлені на іншому.

Можна використовувати неортогональні вейвлети для безперервного вейвлет-перетворення і ортогональні вейвлети для дискретного. При безперервному вейвлет-перетворенні можливе більш детальне вивчення поведінки трафіку. Дискретне перетворення більш корисне для автоматичного виявлення аномалій в мережному трафіку, тому що може працювати швидше і можна встигнути виявляти аномалії мережного трафіку[2].

У загальному випадку, зі збільшенням числа коефіцієнтів вейвлета, функції стають більш гладкими, що може полегшити виявлення мережної атаки. Для виявлення аномалій мережного трафіку необхідно проводити деталізацію інформації з масиву цифрових даних. Тому для вибору системи базисних вейвлетів були проаналізовані вейвлети з компактним носієм: Хаара, Добеши, вейвлети Койфлети, а також Морлі і меськиканський капелюх, які найбільш якісно виділяють локальні особливості сигналів.

Для виконання виявлення мережних аномалій мережного трафіку та шумозаглушення сигналу з використанням різних вейвлет-функцій був використаний пакет Wavelet Tools в програмі Matlab. який має засоби для побудови вейвлет-спектрів сигналів з поліпшеною візуалізацією. Був згенерований мережний трафік з аномаліями і застосовані безперервне і дискретне вейвлет-перетворення з використанням різних вейвлет-функцій для виявлення мережних аномалій. При практичних дослідженнях в розділі Wavelet 1-D пакету Wavelet Tools використано вейвлет Хаара до 10 рівня. Аномалії легко виявлено тільки на 5-9 рівні, краще на 7-9. При використанні вейвлета Добеші другого порядку аномалії теж добре помітні на 7-10 рівнях. В розділі Wavelet Packet 1-D використовувався вейвлет Хаара з максимальним рівнем 8, виявлено аномалії на обраних вузлах кращого дерева після реконструкції. В розділі Continuous Wavelet 1-D результат з використанням Хаара можна бачити в кращому для людського сприйняття вигляді.

Згідно з дослідженнями для моніторингу мережного трафіку доцільно використовувати вейвлет Хаара, і алгоритм Малла для отримання найкращого результату на основі використання вейвлет-перетворення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Введение в вейвлет-преобразование [Text] / А.Н. Яковлев. – Новосибирск, 2003. – 104 с.

2. Дубровін, В.І. Виявлення DOS-атак в мережевому трафіку методом Вейвлет-перетворення [Текст] / В.І. Дубровін, Б.В. Петрик, Г.В. Неласа // Сучасний захист інформації. – 2020. – № 2. – С. 37 – 46.