Микола Дмитрук,
студент 1 СТН курсу спеціальності 208 «Агроінженерія»
Науковий керівник: ***Мушеник Ірина Миколаївна,***
канд. екон. наук, доцент кафедри математичних дисциплін, інформатики і моделювання,
Подільський державний аграрно-технічний університет,
м. Кам'янець-Подільський

СИСТЕМИ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

Інформація протягом історії людства була і є основою для прийняття рішень на рівнях людини, суспільства та держави. У сучасних умовах розвитку інформаційного суспільства інформація розглядається як товар, що має цінність і боротьба за який постійно триває. Попри це, інформація є ефективним інструментом керуючого впливу на соціальні системи – людину, суспільні групи, суспільство за схемою «керуючий вплив – бажаний результат» [1].

Як наслідок, інформація є важливим фактором у формуванні безпечного середовища як з точки зору людських відносин, так і забезпечення громадської, національної і міжнародної безпеки. У свою чергу, інформаційне протиборство – це природній стан в умовах конкуренції сучасного глобалізованого світу, а питанням забезпечення інформаційної та кібернетичної безпеки приділяється особлива увага в контексті збереження балансу інтересів на рівнях особи, суспільства, держави та міжнародного правопорядку.

Стан розвитку інформаційного суспільства й інформаційної інфраструктури України визначає професійні вимоги державних і приватних структур на підготовку фахівців з питань захисту інформації й інформаційно-психологічного протиборства технічних і гуманітарних спеціалізацій. Зазначені напрями професійної діяльності суттєво розвиваються в останні три десятиліття, а сфера кібербезпеки, починаючи з 2000-х років (при цьому поняття національної системи кібербезпеки в Україні законодавчо визначено лише у 2016 році). Відповідно, понятійно-категоріальний апарат професійної

діяльності у сфері кібербезпеки не є остаточно визначеним як на законодавчому, так і практичному і науковому рівнях [2].

Забезпечення інформаційної безпеки є першочерговим завданням кожної держави. В епоху комп'ютеризації і автоматизації проблема комп'ютерної безпеки виходить на перший план. Одним із завдань, яке доводиться вирішувати в контексті інформаційної безпеки є захист інформації, яка зберігається, обробляється і передається в комп'ютерних системах і мережах. Однією із загроз комп'ютерної безпеки є мережеві атаки. Під мережевою (або хакерською) атакою розуміється інформаційний руйнівний вплив, який здійснюється програмним методом і спрямований на розподілену обчислювальну систему [1].

У залежності від методу організації мережевої атаки і засобів, які використовуються виділяють кілька різновидів мережевих атак - DoS, U2R, R2L і Probe (докладний опис кожного з різновиду атак представлений нижче). Існують два напрямки забезпечення комп'ютерної інформаційної безпеки. Першим напрямком є запровадження адміністративних та кримінальних покарань за вчинення комп'ютерних злочинів. Другим напрямком є розробка апаратно-програмних засобів виявлення і захисту від мережевих вторгнень і шкідливих програм [4].

Виявлення мережевих атак на комп'ютерну систему відбувається за допомогою аналізу мережевого трафіку – дані, які надходять в систему або відправляються з неї. Для ясності процесу виявлення розглянемо параметри мережевого трафіку, які аналізуються для забезпечення безпеки комп'ютерних систем, а також типи мережевих атак.

У самому простому випадку система захисту від мережевих атак може представляти собою міжмережевий екран (firewall), він же брандмауер [2, 3]. Мережевий екран – це програмний чи апаратний засіб фільтрації мережевого трафіку за допомогою аналізу його параметрів, таких як адреси джерела і приймача, типів мережевих протоколів і служб, і т.д. Головною відмінністю мережевого екрану від системи виявлення вторгнень є те, що в ньому відсутній

аналіз вмісту переданих пакетів. Відповідно, мережеві екрани мають високу швидкість обробки вхідних і вихідних мережевих пакетів, і працюють, як правило, ґрунтуючись на наборі правил. Недоліком таких систем є низький рівень захисту, що надається, оскільки відсутній аналіз вмісту пакетів [4].

Система виявлення вторгнень (Intrusion Detection System – IDS) на сьогоднішній день є невід'ємною частиною системи безпеки будь-якої комп'ютерної системи, підключеної до локальної або глобальної комп'ютерної мережі. IDS, як правило, це програма або апаратний засіб, який є «фільтром», знаходиться між комп'ютерною системою та комп'ютерною мережею, і аналізує параметри вхідного і вихідного трафіку з метою виявлення фактів несанкціонованого доступу. IDS перехоплює весь мережевий трафік і аналізує вміст кожного пакета на наявність шкідливих компонентів. Крім явних переваг, існуючі системи виявлення вторгнень мають ряд істотних недоліків. А саме: а) вони мають високу ресурсомісткість, через це не завжди є можливість обробляти і аналізувати усі мережеві пакети, що призводить до пропуску атаки; б) не здатні аналізувати зашифровану інформацію; в) мають слабкі можливості виявляти нові типи атак, г) вимагають певного рівня знань в галузі безпеки; д) високий рівень помилок, коли нормальне з'єднання приймається за атаку і навпаки [2].

Штучна нейронна мережа (ШНМ) є математичною (а також програмною або апаратною) моделлю, побудованою за принципом організації та функціонування біологічних нейронних мереж. Сьогодні існує кілька архітектур штучних нейронних мереж, які з успіхом застосовуються для вирішення складних технічних і економічних завдань. Деякими з особливостей ШНМ є здатність в процесі навчання виявляти складні залежності між вхідною і вихідною інформацією, яка була відсутня в навчальній вибірці, і, здатність коректно класифікувати зашумлені образи. Нейронні мережі мають ряд переваг, які вигідно відрізняють їх від традиційних рішень. Деякі з них: висока ступінь паралелізму обробки інформації; здатність до узагальнення, адаптація

до змін навколишнього середовища; розпізнавання зашумлених образів; низький рівень ресурсоємності і т.д.

Для кожного типу мережевої атаки, а їх налічується 22 типи, формується окремий нейромережевий детектор. Для навчання запропонованого нейромережевого детектора використовується навчальна вибірка, що складається з 80% з'єднань одного з типів атак і 20% нормальних з'єднань. Результати експериментів показали, що найкращий відсоток здатності до навчання відбувається, коли навчання проводиться на 32 з'єднаннях мережевої атаки і 8 з'єднаннях легітимного, нормального трафіку [3].

Запропонований підхід, заснований на застосуванні методу нейронних мереж в якості детекторів мережевих атак, дозволяє підвищити рівень виявлення мережевих вторгнень на комп'ютерні системи. Виявлення деяких типів атак відбувається з 100% ймовірністю при незначному рівні помилкових виявлень. Крім цього, запропонований підхід не вимогливий до ресурсів системи і здатний виявляти невідомі типи атак (детектори, яких навчають, на одному типі атак, часто показують хороші результати виявлення інших типів атак, тобто на тих даних, на яких навчання не проводилося.

Список використаних джерел:

1. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: монографія. Запоріжжя : ГУ "ЗІДМУ", 2003. 250 с.

2. Горбуль Д. В., Мушеник І. М. Сучасні електронні технології як інструменти формування інформаційно-освітнього середовища. *Інформаційне суспільство в умовах глобалізації* : зб. наукових праць Всеукраїнської науково-практичної інтернет-конференції, м. Кам'янець-Подільський, 12 травня 2020 р. Кам'янець-Подільський, 2020. С. 152-157.

3. Литвинюк А. А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування. URL: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf

4. Мушеник І. Сучасні реалії і тенденції розвитку інформаційних технологій в освіті. *InterConf.* 2020. Вип. 27. С. 143-146.