ІНТЕЛЕКТУАЛЬНА СИСТЕМА ВИЯВЛЕННЯ АТАК В ЛОКАЛЬНИХ МЕРЕЖАХ

Шпінарева І.

Інструменти виявлення атак мають дуже широкий спектр рішень, від застосування правил, отриманих досвідом, до використання методів машинного навчання, включаючи кілька методів біологічного натхнення. Задачі забезпечення безпеки корпоративних інформаційних систем традиційно вирішується шляхом побудови системи інформаційної безпеки, де одним з найважливіших аспектів безпеки є безпека локальної комп'ютерної мережі.

Станом на сьогоднішній день, кількість нових атак на корпоративні комп'ютерні мережі зростає кожного дня шляхом вторгнення у них за допомогою підключення до інтернету. У зв'язку з чим існуючи системи не завжди здатні виявити наявність атаки і вимагають застосування нових методів і підходів до виявлення атак. В роботі спроектована система виявлення аномальної поведінки мережі за допомогою двох нейронних мереж – перша мережа перевіряє наявність атаки, друга мережа класифікує атаку у разі її наявності.

Ключові слова. Інформаційна безпека, виявлення вторгнення, штучна нейронна мережа, KDD, машинне навчання TCP/IP.

ВСТУП

З самого початку передачі інформації за допомогою комп'ютерних мережевих ресурсів, були розглянуті питання про загрози безпеки інформаційної системи за допомогою різних методів, найбільш часто використовуваних у системах виявлення атак[1].

Аналітичні дані компаній [2], що спеціалізуються в сфері захисту інформації, таких як McAfee, Symantec, Trustware і Kaspersky Labs, показують, що протягом 2018 року стабільно зростала кількість інцидентів, пов'язаних зі спробами порушення безпеки інформаційних систем. Крім цього, спостерігається відносно стабільний ріст кількості нових зразків атакуючих дій. Згідно з міжнародним дослідженням EY в даній області [3], кількість атак різних типів зросла у середньому на дев'ять відсотків у період 2017-2018 рр. Ці дані показують, що існуючі системи виявлення атак не можуть виявляти нові атаки і нові різновиди атак, та вимагають розробку нових методів для покращення результатів виявлення. Сучасні системи виявлення атак повинні виконувати розподілений збір і аналіз інформації, а також інтелектуальний її аналіз.

Станом на сьогоднішній день, існують два класи методів виявлення атак – метод зловживання та метод аномалій. Виявлення атак методами зловживання виконується за допомогою правил, отриманих на основі досвіду або з використанням алгоритмів машинного навчання

відповідно до наборів даних, сигнатур, отриманих з мережевих сценаріїв зі звичайним трафіком, і за допомогою ін'єкційних атак до одного і того ж сценарію. Цей клас методів використовують сучасні системи виявлення атак доповняючи його аналізом мережі у якої вони застосовуються.

Метою роботи є розробка та реалізація системи виявлення вторгнень яка може задовольнити наступні вимоги: система повинна виявляти погрозу застосовуючи методи аномалій; мати низьку ймовірність помилково-позитивних та помилково-негативних результатів; вміти виявляти нові різновидності однієї атаки.

ОГЛЯД МЕТОДІВ АНОМАЛІЙ

A. Аналіз методів аномалій

Методи аномалій засновані на використанні інформації про "нормальну" поведінку системи та її порівнянні з параметрами спостережуваної поведінки. Вони орієнтовані на побудову моделі штатного, або нормального, функціонування системи або користувача. До таких методів відносять:

1) *поведінкові методи:* Вейвлет-аналіз, статистичний аналіз, аналіз ентропії, спектральний аналіз, фронтальній аналіз та кластерний аналіз.

Переваги цих методів полягають у можливості визначити розподілені атаки, в тому числі і в часі, визначити взаємозв'язок між різними подіями, а також кореляція подій дозволяє визначити значущі події серед досліджуваних.

До недоліків цих методів відносять проблему чутливості методів, яка залежить від заданої величини відхилень, точності моделі штучної мережі та ці методі дуже сильно залежать від функції подібності [4].

2) *методи машинного навчання:* Дерево рішень, Баєсова мережа, MAP-сплайни, алгоритми кластеризації та алгоритми регресії.

До переваги цих методів відносять легкість реалізації, низькі вимоги до підготовки даних, малий час обробки великої кількості даних і використовують модель білого ящика, що допомагає перевірити модель з використанням статистичних тестів.

Недоліками цих методів є проблема навчання, що вимагає ретельного підбору коефіцієнтів та проблема побудови оптимальних моделей.

3) *методи обчислювального інтелекту:* Нейронні мережі, генетичні алгоритми, нечітка логіка, імунні системи, метод опорних векторів та ройові алгоритми.

Перевагами цих алгоритмів є можливість бистрої обробки великої розмірності даних, також у паралельному режимі, легкі для реалізації, добре працюють навіть на поганому наборі даних та здатні вирішувати нелінійні задачі [5].

Недоліками методів є потрібність як у позитивних, так і негативних прикладах, вони вимагають багато пам'яті і процесорного часу, потребують виборі оптимальної функції ядра або активації.

Враховуючи ці особливості, було вирішено використовувати нейронні мережі типу – багатошаровий перцептрон Румельхарта, та навчати їх алгоритмом зворотного поширення помилки.

БАЗА ДАНИХ ДЛЯ АНАЛІЗУ АТАК

NSL-KDD – це набір даних, запропонований Тавалае та ін.[6]. Набір даних NSL-KDD є скороченою версією оригінального набору даних KDD 99. Він складається з тих самих функцій, що і KDD 99, 41 змінна та одного атрибуту класу. Атрибут класу має 21 значення, що потрапляють під чотири типи нападу: Probe attack, User to Root (U2R), Remote to Local (R2L) та атаки Denial of Service (DoS). Цей набір даних має атрибут дворядкового класу.

Таблиця I. Класи і приклади типів атак

Клас атак	Тип атак
DoS	Back, Land, Neptune, Pod, Smurf, Teardrop, Apache2, Udpstorm, Processtable, Worm
Probe	Satan, Ipsweep, Nmap, Portsweep, Mscan, Saint
R2L	Guess_Password, Ftp_write, Imap, Phf, Multihop, Warezmaster, Warezclient, Spy, Xlock, Xsnoop, Snmpguess, Snmpgetattack, Httptunnel, Sendmail, Named
U2R	Buffer_overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm, Ps

Нижче представлені короткі описи атак:

− DOS. Відмова в обслуговуванні є атакою, яка виснажує ресурси жертви, тим самим роблячи її нездатною обробляти нормальні запити.

− Probing. Мета атаки полягає в віддаленому спостереженні і зборі інформації про жертву.

− U2R. Даний тип атак, використовує доступ до існуючого облікового запису користувача в комп'ютерній системі жертви, отриманий, наприклад, методами соціальної інженерії, щоб, використовуючи вразливості, отримати доступ до облікового запису суперкористувача.

− R2L. Неавторизований доступ з віддаленого комп'ютера дозволяє зловмисникові увійти в віддалену машину і отримати локальний доступ до комп'ютера.

Кожна з представлених атак, по суті своїй, є цілим класом, кожен з яких включає в себе безліч конкретних прикладів (табл. I).

Крім того, в NSL-KDD є достатня кількість навчальних та тестових прикладів, що робить можливим проведення експериментів.

A. Опис бази даних виявлення вторгнень

Записи з NSL-KDD, що використовуються для навчання та тестування, складаються з двох основних компонентів: перший з них являє собою набір функцій що описують подію, а другий це клас, який інформує тип події, тобто якщо це нормальна або ненормальна поведінка, всі ці зразки організовані у файлі CSV.

B. Атаки без контенту

У деяких атаках надсилається інформація вище 4-го рівня моделі OSI, щоб скористатися вразливістю програми, тому довжина корисного навантаження четвертого рівня відрізняється від нуля. Таки типи нападів зазвичай називають "атаками на основі контенту" [7].

З іншого боку, є деякі атаки, яким не потрібно надсилати інформацію на рівень сеансу або вище, це означає, що корисний набір можливого пакету четвертого рівня порожній, ці напади будуть називатися атаками без контенту.

Оскільки аналізується трафік локальної комп'ютерної мережі, отримати інформацію про зміст атаки, а точніше, зміст переданого пакета по мережі немає можливості, в слідстві чого, потрібно проаналізувати існуючий набір атак і вибрати характеристики, які не пов'язані із вмістом атаки. З 41 доступних змінних, 13 на основі контенту, це означає, що такі дані не є необхідними для виявлення атак, не пов'язаних з контентом.

Найважливішою особливістю при виявленні атак без контенту є прапор статусу з'єднання, тобто 4-а особливість в наборі даних. Найважливіші можливі стани прапору статусу наведені в табл. 2.

Історичні події можуть допомогти в процесі виявлення, бо деякі атаки зазвичай приймають різні кроки, щоб бути успішними. Аналізуючи кроки, можна дізнатись, що в мережевому трафіку трапляється щось не так, наприклад, в атаці з портів, можна знайти запити, які надходять до не пропонованої служби, викликаючи з'єднання з режимом REJ, це не обов'язково означає, що присутня атака на порти portsweep, а можливо, що хтось намагається отримати інформацію про послуги, що пропонуються в мережі.

Таблиця 2. Флаг стану з'єднання

Стан	Значення
SF	Нормальне SYN/FIN завершення
REJ	З'єднання відхиллено, початковий SYN викликав відповідь RST
S0	Стан 0: відправив SYN, відповіді нема
S1	Стан 1: з'єднання встановлено (обмінялись SYN), більше ніякої активності
S2	Стан 2: з'єднання встановлено, ініціатор закрив свою сторону
S3	Стан 3: з'єднання встановлено, відповідач закрив свою сторону
RSTO RSTR OTH	Ініціатор оновлює з'єднання Відповідач оновлює з'єднання Друге, цей стан не підтримується.

Через характер нападів на комп'ютерну мережу були обрани усі характеристики, зокрема характеристик 10-22, ці характеристики відносяться до атак з контентом. Описи кожної характеристики можна знайти в [8].

МОДУЛІ СИСТЕМИ

Створена система здатна збирати інформацію з мережевого інтерфейсу. Архітектура системи представлена на рис.I.

Модуль сенсору складається з застосування утиліти Tshark [9]. На момент початку роботи, система починає процес Tshark, та кожні 30 секунд зберігає трафік мережі в обраної папці. Збір даних здійснюється за протоколами TCP, UDP і ICMP. При запуску цього модулю, запускається робота модуля аналізатора пакетів, який інтерпретує збережені пакети у форматі XML, після чого збирає інформацію про пакети та передає аналізатору з'єднань. Аналізатор з'єднань отримує пакети, та в залежності від прапорів, встановлених в пакеті, вирішує чи встановити нове з'єднання, оновити інформацію вже існуючого або треба видалити з'єднання. Модуль аналізатору з'єднань відстежує стан з'єднання по описаним прапорам в табл. 2, при установленні яких, передає інформацію про з'єднання модулю збору статистики, а також, слідкує за часом з'єднання, та виконує роботу двох секундного вікна. Якщо з'єднання було оновлено понад дві секунди тому, дане з'єднання перевіряється на атаку у разі необхідності, після чого видаляється зі списку з'єднань. Збірник статистики при отриманні з'єднання збирає статистичні дані за останні дві секунди та утворює вектор з 28-ми змінними для аналізу на наявність атаки.

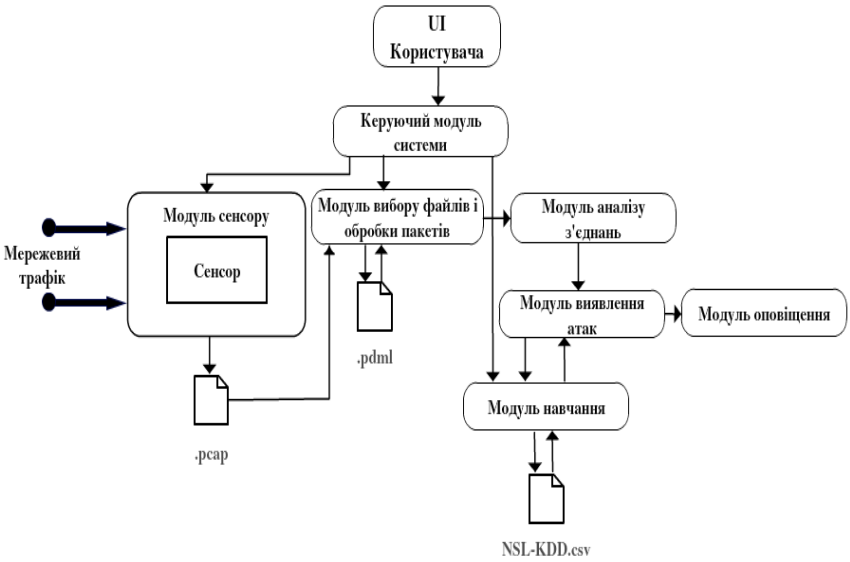

Рис. 1 – Архітектура системи виявлення вторгнень

У якості вихідних даних модуля очікується вектор в форматі NSL-KDD, що складається з наступних полів:

1) Основні характеристики мережевих з'єднань

Duration – Тривалість з'єднання

Protocol_type – Протокол, що використовується при з'єднанні

Service – Цільовий сервіс, що використовується

Flag – Статус з'єднання: нормальне, помилка

Src_bytes – Кількість байтів, переданих від джерела до приймача за одне з'єднання

Dst_bytes – Кількість байтів, переданих від приймача до джерела за одне з'єднання

Land – Якщо джерело та приймач має однакові номери портів, то параметр набуває значення 1, якщо не однакові – 0

Wrong_fragm ent – Загальна кількість пошкоджених фрагментів у конкретному з'єднанні

Urgent – Кількість термінових пакетів у конкретному з'єднанні. Терміновий пакет – це пакет, в якому активований біт терміновості URG

2)Характеристики пов'язані з часом мережевого з'єднання

Count – Кількість під'єднань до цільового хоста протягом часового інтервалу в 2с.

Srv_count – Кількість під'єднань до поточної служби (номеру порта) за останні 2с.

Serror_rate – Відсоток з'єднань з помилкою типу SYN для даного хоста джерела
Srv_serror_rate – Відсоток з'єднань з помилкою типу SYN для даної служби джерела
Rerror_rate – Відсоток з'єднань з помилкою типу REJ для даного хоста джерел
Srv_rerror_rate – Відсоток з'єднань з помилкою типу REJ для даної служби джерела
Same_srv_rate – Відсоток з'єднань зі службою
Diff_srv_rate – Відсоток з'єднань з різними службами
Srv_diff_host_ rate – Відсоток з'єднань з різними хостами

3)Характеристики пов'язані з хостом мережевого з'єднання

Dst_host_coun t – Кількість з'єднань з хостом
Dst_host_srv_ count – Кількість з'єднань зі службою
Dst_host_same_srv_rate – Відсоток з'єднань з даною службою на даному хості
Dst_host_diff_ srv_rate – Відсоток з'єднань з різними службами на даному хості
Dst_host_same_src_port_rate – Відсоток з'єднання з даним хостом при поточному номері порта джерела
Dst_host_srv_ diff_host_rate – Відсоток з'єднань зі службою різних хостів
Dst_host_serror_rate – Відсоток з'єднань з помилкою типу SYN для даного хоста приймача
Dst_host_srv_serror_rate – Відсоток з'єднань з помилкою типу SYN для даної служби приймача
Dst_host_rerror_rate – Відсоток з'єднань з помилкою типу REJ для даного хоста приймача
Dst_host_srv_r error_rate – Відсоток з'єднань з помилкою типу REJ для даної служби приймача

Виявлення «аномальної» поведінки системи здійснюється модулем аналізу атаки. Модуль аналізу атаки містить у собі каскад з двох нейронних мереж. Ідея каскаду НМ полягає в розподілі головної задачі системи виявлення атак на кілька малих задач, які вирішуються різними нейронними мережами. Головною задачею системи являється виявлення атак і їх класифікація. Перша мережа аналізує на наявність атаки, друга мережа класифікує тип атаки. Але, оскільки перша задача вирішує питання наявності атаки, а нейронні мережі мають недолік помилкового спрацьовування, то друга нейронна мережа крім класифікації відомих атак буде перевіряти результати першої нейронної мережі на наявність атаки або на розпізнавання невідомих атак. Цій варіант також дає подвійну перевірку від помилково-позитивних результатів системи. Модуль нейронної мережі являє собою конструктор

для створення багатошарової нейронної мережі – багатошаровий перцептрон. Нейронні мережі мають три шари. Перший – шар вхідних параметрів, який має розмір 28, другий – схований шар, який має розмір 84 та третій – вихідний шар, який має розмір 2 або 5, відповідно до типу мережі. Система розпізнає такі класи атак: DOS (Denial of service), Probing, R2L (Remote to local attack), U2R (User to root). Система працює у двох режимах, перший режим – режим налаштування, який навчає кожну нейронну мережу, другий режим –- аналіз трафіку у реальному часі.

ТЕСТУВАННЯ

A. Метрика для оцінки якості

Для порівняння продуктивності і ефективності методів виявлення вторгнень в мережі використовуються такі метрики [10]: ймовірності істинно-позитивних (True Positive Rate, TPR) та помилково-позитивних результатів (False Positive Rate, FPR). FPR є ймовірністю отримати оповіщення у разі перевірки нормальної поведінки. До того, ймовірність помилково-негативного рішення (False Negative Rage, FNR) означає, що система не видає оповіщення у разі наявності зловмисної поведінки. Рівняння (1) та (2) відображують FPR та FNR.

$$\mathbf{FPR} = \frac{number\ of\ false\ positive}{number\ of\ negative}. \quad (1)$$

$$\mathbf{FNR} = \frac{number\ of\ false\ negative}{nuimber\ of\ positive}. \quad (2)$$

Звідси, ймовірність TPR та істинно-негативних результатів (True Negative Rate, TNR) дорівнюють:

$$TPR = 1 - FNR \quad \text{та}$$
$$TNR = 1 - FPR \quad (3)$$

Також, до цих показників можна додати ймовірність правильної класифікації (True Rate, TR) і ймовірність помилкової класифікації (False Rate, FR).

$$TR = \frac{number\ of\ true\ positive + number\ of\ true\ negative}{number\ of\ psitives + number\ of\ negatives} \quad (4)$$
$$FR = 1 - TR.$$

Рівняння (5) відображує міру чутливості (sensitivity), вона визначається як частка нормальної поведінки:

$$\mathbf{Sensitivity} = \frac{number\ of\ true\ positives}{number\ of\ true\ positives + number\ of\ false\ negatives} \quad (5)$$

Але, ця міра недостатньо змістовна, оскільки вона може бути тривіально досягнута шляхом класифікації всієї поведінки як зловмисної. Ще одна метрика, міра специфіки (specificity). Це частка справжніх негативів всієї розглянутої негативної поведінки:

$$\text{Specificity} = \frac{number\ of\ true\ negatives}{number\ of\ true\ negatives + number\ of\ false\ positives} \quad (6)$$

При класифікації всього трафіку як нормального, міра специфіки досягається повністю. F-міра є показником, що поєднає міри чутливості та специфіки:

$$\mathbf{F-measure} = \frac{\mathbf{2 \times sensitivity \times specificity}}{\mathbf{sensitivity + cpecificity}} \quad (7)$$

A. Тестування різних нейронних мереж

Тестування і вибір розміру, функції активації та показника навчання проводились у ОС Windows® 10-64 з процесором Intel Core i7 2600k (3.4 GHz), 12,0 Гб ОЗУ. Реалізація нейронних мереж була створена за допомогою Microsoft CNTK[11], та система була реалізована на мові C#. Навчання НМ здійснюється методом зворотного поширення помилки. Точність розбіжності очікуваного і отриманого результатів визначається автоматично завдяки бібліотеці CNTK, яка виконує ітеративний прохід засновуючись на отриманої кількості ітерацій 300 і мінібатчами по 64 вектора. Система виявлення атак була навчена на виборці NSL-KDD на 133,504 векторах та протестована на 15040. Сама вибірка векторів мала 95% варіації, та кожен вектор унікальний, тобто навчальна та вибірка для тестування не мають однакових векторів.

Каскад складається з двох нейронних мереж. Перша нейронна мережа, повинна встановлювати, чи є наявність атаки, друга повинна встановлювати клас атаки. Тобто, перша нейронна мережа на виході у якості результату надає вектор з двох значень – є атака чи ні, друга нейронна мережа у якості відповіді надає вектор з п’ятьма значеннями – Probe, R2L, U2R, DoS та «не є атакою». Перші значення відповідають класам атак, а остання застосовується для подвійної перевірки, якщо перша нейронна мережа помилково вирішила що зв’язок небезпечний.

Для ефективного знаходження мережевих атак необхідно вибрати структури нейронних мереж, використованих у каскаді. Для вибору структури нейронних мереж були протестовані п’ять функцій активації з різними коефіцієнтами навчання та кількості шарів. Таблиця III відповідає трьох шаровим нейронним мережам з коефіцієнтом навчання 0.02. Перший шар відповідає 28 змінним які передає система, другий шар містить кількість нейронів кратну трьом(84), або п’яти(140), та останній шар містить два, якщо це перша нейронна мережа та п’ять, якщо друга. Кількість нейронів у другому шарі було обраний емпіричним шляхом у

ході тестування. Кількість шарів нейронних мереж дорівнює трьом, при спробі збільшення їх кількості, показники точності значно падали.

Перша нейронна мережа показала найкращій результат за показниками Tr, Fr, TPR, FNR, Recall та F-measure з функцією активації ReLU та середнім шаром розміром 84 (табл.3). Цю нейронну мережу було обрано для починання каскаду.

Таблиця 3. Оцінка якості першої нейронної мережи (28/84/2) з різними функціями активації та η=0,02

	Tr	Fr	TPR	TNR	FPR	FNR	Recall	Precision	F-measure
Tanh	95.47	4.53	97.44	93.39	2.56	6.61	93.39	97.44	95.37
ReLU	96.30	3.70	97.34	95.21	2.66	4.79	95.21	97.34	96.26
Sigmoid	95.35	4.65	97.68	92.87	2.32	7.13	92.87	97.68	95.22
ELU	95.70	4.30	96.93	94.40	3.07	5.60	94.40	96.93	95.65
SELU	95.04	4.96	96.97	92.99	3.03	7.01	92.99	96.97	94.94

Друга нейронна мережа показала більш розподілений результат. Нейронна мережа з функцією активації ReLU та з середнім шаром розміром 140 видає кращій результат за показниками TPR(96,38%), FPR(3,6%), Recall (95%) та F-measure(96,32%), а нейронна мережа з середнім шаром розміром 84 видає кращій результат за показниками Tr та Fr. Оскільки головними для нас є показника Tr та Fr, у якості другої нейронної мережі була обрана мережа з функцією активації ReLU, середнім шаром розміром 84 та коефіцієнтом навчання η=0.02 (табл.4).

Таблиця 4. Оцінка якості другої нейронної мережи (28/84/5) з різними функціями активації та η=0,02

	Tr	Fr	TPR	TNR	FPR	FNR	Recall	Precision	F-measure
Tanh	95.94	4.06	98.35	93.36	1.65	6.64	93.36	98.35	95.79
ReLU	96.02	3.98	98.10	93.81	1.90	6.19	93.81	98.10	95.90
Sigmoid	95.60	4.40	98.66	92.32	1.34	7.68	92.32	98.66	95.39
ELU	95.85	4.15	98.51	93.01	1.49	6.99	93.01	98.51	95.68
SELU	95.54	4.46	97.75	93.18	2.25	6.82	93.18	97.75	95.41

Також кожна нейронна мережа була протестована з коефіцієнтом навчання 0.04 або 0.08 та з більшою кількістю шарів. При використанні трьох шарів та коефіцієнту навчання η=0.04, показники Tr та Fr мають гірший результат у середньому на 0.3 відсотка, а при збільшення коефіцієнту навчання цей показник значно зростає, проте, при збільшенні кількості шарів та використанні коефіцієнту навчання 0.02, показники Tr та Fr відрізняються вже на 10,3 відсотки у середньому.

Таблиця 5 демонструє порівняння між обраними нейронними мережами першого і другого типу окремо, та створений з них каскад, ReLU_1 – нейронна мережа першого типу, відповідно ReLU_2 –

нейронна мережа другого типу. Як можна бачити з таблиці, каскад з цих мереж показав кращий результат за показниками Tr, Fr, TNR, FNR та Precision. Це показує, що створений каскад в загалі краще працює, а також має нижчу ймовірність прийняти безпечний трафік за небезпечний. Покращити показники TPR та FPR можна при підвищенні показників першої нейронної мережі.

Таблиця 5. Порівняння якості каскаду

	Tr	Fr	TPR	TNR	FPR	FNR	Recall	Precision	F-measure
ReLU_1	96.38	3.62	97.65	94.96	2.35	5.03	95.03	97.65	96.32
ReLU_2	96.31	3.69	97.49	94.46	2.51	5.53	95.05	97.49	96.25
Casscade	**96.91**	**3.09**	**98.69**	**96.78**	**1.31**	**3.21**	**96.78**	**98.7**	**97.73**

ВИСНОВКИ

Перспективними напрямками при проектуванні систем виявлення атак в даний час бачиться використання методів машинного навчання і гібридизація підходів, яка дозволила б поєднувати в собі переваги сигнатурних і евристичних методів, а також використання технологій великих даних і проактивного моніторингу безпеки. Одним з основних вимог, що пред'являються до цих рішень, є забезпечення адаптивної і високо масштабованої аналітичної обробки подій, що забезпечує інтелектуальне управління великими обсягами даних про безпеку в реальному або близькому до реального масштабі часу

Метою роботи було створити систему аналізу інтернет трафіку для виявлення атаки на локальну комп'ютерну мережу. В роботі для виявлення інформативних ознак атак були розглянути нейронні мережи прямого поширення з різними фунуціями активації та кількості шарів, на підставі яких був створен каскад нейронних мереж у якості нового засобу аналізу даних трафіку. Запропонований каскад показав кращий результат – 96.91 відсотків, ніж використання кожної нейронної мережі окремо, та була створена система аналізу мережевого трафіку для виявлення атак.

Система була протестована на локальній мережі що містить 14 комп'ютерів. На локальну мережу була імітована DoS атака у розмірі 26,102 пакетів, 93.41% з яких було корректно ідентіфіковано як атаку.

ЛІТЕРАТУРНІ ДЖЕРЕЛА

[1] Nikishova A., Churilina A. Distributed intrusion into information system of entherprise detection Izvestiya UFU, Technical science, 2013. – №12 (149).
[2] Information Security Threats, www.anti-malware.ru/threats/information-security-threat.
[3] Garuba, M.; Chunmei Liu; Fraites, D.; "Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems," Information Technology: New Generations, 2008. ITNG 2008. Fifth International

Conference on. – no. 7-9. – P.592 – 598, DOI: 10.1109/ITNG.2008.231.
[4] A. A. Branitsky, I. V. Kotenko, “Analysis and classification of methods for detecting network attacks”, Tr. SPIIRAN, 45 (2016). – P. 207 – 244.
[5] I.M. Shpinareva «The comparative characteristic of the intrusion detection systems on basis of neural networks»/ Book of abstracts of the International Scientific Conference “Computer Algebra and Information Technology” / 20-26 August 2012, Odessa.- P. 86 – 89.
[6] Tavallaee, M.; Bagheri, E.; Wei Lu; and Ghorbani, A.A detailed analysis of the KDD CUP99 data set. Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009). – P.1– 6.
[7] Pasupulati, A.;Coit, j.; Levitt, K; Wu, S.F.; Li, S.H.;Kuo, J.C.; Fan, KP.; "Buttercup: on network-based detection of polymorphic buffer overflow vulnerabilities," Network Operations and Management Symposium, 2004. NOMS 2004. IEEE/IFIP. – Vol.1. – P.235 – 248.
[8] Dhanabal, L. and Dr. S. P. Shantharajah. “A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms.” 2015. Tshark [Електронний ресурс] – Режим доступу: http://www.wireshark.org/ docs/man-pages/tshark.html.
[9] Holz T. 13 security measurements and metrics for networks, Dependability Metrics, 2008. – P. 157 – 165. DOI: 10.1007/978-3-540-68947-8_13
[10] CNTK [Електронний ресурс] – Режим доступу: https://www.microsoft.com/ en-us/cognitive-toolkit
[11] Lukatsky A.V. Obnaruzhenie atak [Attack Detection]. SPb.: BHV-Petersburg, 2003. – 608 p.

INTELLECTUAL SYSTEM FOR DETECTION ATTACK IN LOCAL NETWORKS

Spinareva I.

Attack detection tools have a very wide range of solutions, from applying the rules of experience to using machine learning methods, including several biological inspiration methods. Corporate information systems security has traditionally been addressed by building an information security system where one of the most important aspects of security is the security of the local area network. As of today, the number of new attacks on corporate computer networks is increasing every day by invading them through an internet connection. Therefore, existing systems may not always be capable of detecting an attack and require the use of new methods and approaches to detecting attacks. The system designed to detect anomalous behavior of the network using two neural networks - the first network checks for an attack, the second network classifies the attack if it exists.

Keywords. Information Security, Intrusion Detection, Artificial Neural Network, KDD, TCP / IP Machine Learning. Correction