ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ

УДК 004.056.53:[004.7:004.032.26]

І. В. ЖУКОВИЦЬКИЙ[1*], В. М. ПАХОМОВА[2*], Д. О. ОСТАПЕЦЬ[3*], О. І. ЦИГАНОК[4*]

[1*]Каф. «Електронні обчислювальні машини», Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпро, Україна, 49010, тел. +38 (056) 373 15 89,
ел. пошта ivzhukl@ua.fm, ORCID 0000-0002-3491-5976
[2*]Каф. «Електронні обчислювальні машини», Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпро, Україна, 49010, тел. +38 (056) 373 15 89,
ел. пошта viknikpakh@gmail.com, ORCID 0000-0002-0022-099X
[3*]Каф. «Електронні обчислювальні машини», Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпро, Україна, 49010, тел. +38 (056) 373 15 89,
ел. пошта odaua@i.ua, ORCID 0000-0003-1778-7770
[4*]Каф. «Електронні обчислювальні машини», Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпро, Україна, 49010, тел. +38 (056) 373 15 89,
ел. пошта tsiganok.oleg@yandex.ua, ORCID 0000-0001-9846-7669

ВИЯВЛЕННЯ АТАК НА КОМП'ЮТЕРНУ МЕРЕЖУ НА ОСНОВІ ВИКОРИСТАННЯ КОМПЛЕКСУ НЕЙРОННИХ МЕРЕЖ

Мета. За основну мету дослідження ми ставимо розвиток методики визначення атак на комп'ютерну мережу. Досягнення поставленої мети передбачає вирішення таких завдань: розробити методику виявлення атак на комп'ютерну мережу на основі ансамблю нейронних мереж із використанням нормалізованих даних відкритої бази KDDCup99; під час виконання машинного навчання виявити оптимальні параметри нейронної мережі, що забезпечить достатньо високий рівень достовірності виявлення вторгнень у комп'ютерну мережу. **Методика.** Як архітектурне рішення модуля виявлення атак запропоновано дворівневу мережну систему, основу якої складає ансамбль із п'яти нейронних мереж типу багатошарового персептрона: перша нейронна мережа – для визначення категорії класу атаки (DoS, R2L, U2R, Probe) або факту того, що атаки не було; інші нейронні мережі – для виявлення типу атаки, якщо така мала місце (кожна з цих чотирьох нейронних мереж відповідає одному класу атаки і вміє визначати типи, що належать тільки цьому класу). **Результати.** На створеній програмній моделі проведено дослідження параметрів нейронної мережі конфігурації 41–1–132–5, яка визначає категорію класу атаки на комп'ютерну мережу. Встановлено, що оптимальна швидкість навчання дорівнює 0,001. Для оптимізації найкраще себе показав алгоритм ADAM. Як функція активації для прихованого шару найбільше підходить функція ReLU, для функції активації вихідного шару – функція гіперболічного тангенса. Точність на тестовій та валідаційній вибірках склала 92,86 та 91,03 % відповідно. **Наукова новизна**. Розроблена програмна модель, для якої використана мова програмування Python 3.5, інтегроване середовище розробки PyCharm 2016.3 та фреймворк Tensorflow 1.2, дає можливість виявляти всі типи атак класів DoS,U2R, R2L, Probe. **Практична значимість**. Отримано графічні залежності точності нейронних мереж за різних параметрів: швидкості навчання; активаційної функції; алгоритму оптимізації. Визначено оптимальні параметри нейронних мереж, що забезпечать достатньо високий рівень достовірності виявлення вторгнень у комп'ютерну мережу.

Ключові слова: архітектурне рішення; нейронна мережа; швидкість навчання; функція активації; алгоритм оптимізації

doi: https://doi.org/10.15802/stp2020/218318

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)

Вступ

Ефективність функціонування сучасних інформаційних систем у значній мірі пов'язана з проблемою захисту оброблюваної в них інформації. Згідно зі звітом Verizon 2018 Data Breach Investigations Report [14], проблема виявлення вторгнень є актуальною. Із року в рік значення середньої вартості зламу збільшується на 6 %. Існує велика кількість алгоритмів класифікацій та виявлення аномалій, кожен із яких має свої переваги та недоліки [11]. Для виявлення нових типів атак також використовують системи виявлення вторгнень на основі аномалій. На базі набору запитів формують модель нормальної поведінки, із якою порівнюють кожен поточний запит до системи.

Можливості наявних систем захисту не дозволяють забезпечити безпеку інформаційної системи на достатньому рівні. Причиною цього є те, що процес створення систем виявлення атак пов'язаний із низкою невирішених науково-технічних завдань. Наявні системи виявлення атак використовують найпростіші алгоритми обробки інформації, яка надходить, що не дозволяє виявити значну кількість атак на інформаційні системи. До основних методів виявлення атак належать виявлення зловживання (misuse detection) і виявлення аномалій (anomaly detection) [11]. Виявлення зловживання передбачає наявність сигнатур атак та базується на простому понятті збігу послідовності зі зразком. Через те що метод виявлення атак на базі сигнатур є статичним, він вразливий до нових типів атак. Для їх виявлення необхідно використовувати системи здатні до самонавчання в реальному часі [6]. Створення ефективної системи виявлення атак вимагає застосування якісно нових підходів до обробки інформації, які повинні ґрунтуватися на адаптивних алгоритмах, здатних до самонавчання. Відомо, що існує два основних види реалізації систем виявлення вторгнень на базі нейронних мереж: IDS (Intrusion-Detection System) на основі комбінації експертної системи та нейронної мережі; IDS із використанням нейронних мереж (НМ) як автономних систем [6]. Найбільш перспективним напрямом у створенні подібних систем виявлення атак є застосування засобів штучного інтелекту. Слід зауважити, що дослідженнями в цьому аспекті займаються як великі закордонні комерційні компанії (Cisco, Computer Associates, ISS, Symantec та інші), так і науково-дослідницькі центри при різних університетах (Columbia University, Florida Institute of Technology, Purdue University, Ohio University, ін.).

Аналіз наукових джерел. Найбільш перспективний напрям представляють IDS, що побудовані на основі НМ: багатошарового персептрона (Multi Layer Perceptron, MLP); радіальнобазисної мережі (Radial Basis Function Network, RBF) та мережі Кохонена або самоорганізаційної карти (Self Organizing Maps, SOM). Так, наприклад, в [10] проаналізовано тільки DDoS-атаки за протоколами TCP, UDP і ICMP через їх популярність серед зловмисників. У [13] здійснено виявлення в мережі деяких загроз на основі аналізу та обробки параметрів мережних з'єднань, що використовують стек протоколів TCP/IP, із використанням нейронної мережі конфігурації 19–1–25–5 (19 – кількість вхідних нейронів; 1 – кількість прихованих шарів; 25 – кількість прихованих нейронів; 5 – кількість вихідних нейронів), але інші типи атак також потребують досліджень.

На сучасному етапі, з одного боку, усе частіше з'являються роботи, що використовують комбінований підхід до розв'язання задачі. Так, наприклад, у [5] запропоновано новий ансамблевий класифікатор, що використовує RBF і нечітку кластеризацію, щоб підвищити точність виявлення, зменшити кількість помилкових спрацьовувань та забезпечити більш високий рівень виявлення для нечастих атак. В [1] розглянуто підхід із використанням нейронних мереж, імунних систем, нейронечітких класифікаторів та їх комбінацій. Сутність гібридних підходів полягає в реалізації різних схем об'єднання базових класифікаторів, які дозволяють ліквідувати недоліки в їх функціонуванні відокремлено. Однак важливим недоліком таких методик є відсутність універсальності їх застосування. У [4] для підвищення ефективності роботи IDS запропоновано використовувати метод збігу, заснований на тому, що НМ із різними топологіями (MLP, RBF, SOM) можуть детектирувати різні атаки, але помилкові спрацьовування також відбуваються не завжди на одних і тих самих мережних пакетах під час аналізу за допомогою різних типів НМ.

doi: https://doi.org/10.15802/stp2020/218318

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)

Крім того, кожний тип нейронної мережі має свої переваги й недоліки, які необхідно враховувати або проводити додаткові дослідження.

З іншого боку, наявні спроби використання НМ на різних рівнях. Так, наприклад, у [2] розглянуто новий підхід до побудови багаторівневої мережної системи виявлення вторгнень, який полягає в тому, що групи однотипних параметрів міжмережної взаємодії подають на входи окремих модулів першого рівня, кожен із яких представляє собою ієрархічну структуру декількох НМ різного типу та виконує виявлення аномалій за заданою групою параметрів. Результати роботи модулів першого рівня надходять на вхід вирішувача другого рівня, що приймає остаточне рішення про наявність атаки та її класифікацію. За таким підходом імовірність визначення відомих атак склала 91 %, виявлення вторгнень, про які не було інформації під час навчання, склала 86 %. Однак розроблений прототип має відносно значну ймовірність помилки II роду – 18 %, аналіз та виправлення причин цих помилок є перспективним для подальшого дослідження.

Крім того, у великих інформаційних системах (зокрема, інформаційно-телекомунікаційній системі залізничного транспорту) виникає ще проблема великого обсягу мережного трафіка, це пов'язано з тим, що мережний трафік постійно змінюється, і досить важко встановити циклічність такої зміни. Для підвищення ефективності виявлення ситуацій, пов'язаних із можливими вторгненнями в комп'ютерну мережу, яка складає основу різних інформаційних систем, останнім часом широко використовують сучасні технології інтелектуального аналізу даних (зокрема, технології DataMining) [8]. Мережні системи виявлення вторгнень на основі парадигми виявлення аномалії мають високу помилкову частоту тривоги, що ускладнює їх використання. Щоб вирішити цю слабкість, у [7] запропоновано згладити виводи детекторів аномалій за допомогою локального адаптивного багатофакторного згладжування.

Ми вважаємо, що під час обробки великого обсягу мережного трафіка, який постійно змінюється, застосування багаторівневої мережної системи виявлення атак різних категорій на основі MLP з використанням машинного навчання (особливо глибокого) призводить до великої кількості помилкових спрацьовувань і пропусків атак. Тому одним із підходів до вирішення такої проблеми є проведення додаткових досліджень для визначення раціональних параметрів НМ.

Мета

У нашому дослідженні поставлено за мету розвиток методики визначення атак на комп'ютерну мережу. Досягнення поставленої мети передбачає вирішення наступних завдань:

– розробити методику виявлення атак на комп'ютерну мережу на основі ансамблю нейронних мереж;

– під час виконання машинного навчання виявити оптимальні параметри нейронної мережі (MLP), що забезпечить достатньо високий рівень достовірності виявлення вторгнень у комп'ютерну мережу.

Методика

Досліджувані матеріали, використані під час моделювання. Розглянуто систему виявлення атак на основі нейронних мереж типу багатошарового персептрона. У роботі [3] автори провели дослідження двох підходів до визначення атак на комп'ютерну мережу та довели раціональність використання ансамблю нейронних мереж. У нашій роботі джерелом даних для навчання та тестування нейронних мереж виступає база даних KDDCup99 [9], що містить понад чотири гігабайти характеристик TCP-підключень. У базі представлено такі категорії атак: DoS, R2L, U2R, Probe. Кожна з цих категорій, у свою чергу, представлена кількома типами.

DoS – мережні атаки, спрямовані на виникнення ситуації, коли в атакованій системі відбувається відмова в обслуговуванні. Такі атаки характеризуються генерацією великого обсягу трафіка, що призводить до перевантаження та блокування сервера. Виділяють шість типів DoS-атак: back, land, neptune, pod, smurf, teardrop.

R2L-атаки характеризуються отриманням доступу незареєстрованого користувача з віддаленого комп'ютера. Виділяють вісім типів R2L-атак: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster.

U2R-атаки передбачають отримання зареєстрованим користувачем привілею локального суперкористувача (мережного адміністратора). Виділяють чотири типи U2R-атак: buffer_overflow, loadmodule, perl, rootkit.

doi: https://doi.org/10.15802/stp2020/218318

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)

Probe-атаки полягають у скануванні мережних портів із метою отримання конфіденційної інформації. Виділяють чотири типи Probe-атак: ipsweep, nmap, portsweep, satan.

Вхідним вектором для системи виявлення атак є набір із 41 параметра TCP-з'єднання, повний опис яких наведено в [9], приклади опису – у табл. 1.

Як архітектурне рішення модуля виявлення атак запропоновано п'ять нейронних мереж типу багатошарового персептрона: НМ1 – для визначення категорії класу атаки (DoS, R2L, U2R, Probe) або факту того, що атаки не було; НМ2…НМ5 – для виявлення типу атаки, якщо така мала місце (кожна з цих чотирьох нейронних мереж відповідає одному класу атаки і вміє визначати типи, що належать тільки цьому класу). На рис. 1 наведена структура гіпотетичного комплексу, який використовує це архітектурне рішення.

Комплекс містить модуль виявлення мережних атак, що отримує дані про з'єднання від мережних датчиків і надає результат до модуля реагування. Сигнал від НМ1, який виявляє категорію класу атаки, через ключ «кл» вмикає одну з нейронних мереж НМ2…НМ5, яка визначить тип атаки цього класу.

Таблиця 1

Опис параметрів TCP-з'єднання

№	Назва	Опис	Тип
1	duration	тривалість з'єднання (с)	числовий
2	protocol_type	тип протоколу (TCP, UDP тощо)	символьний
3	service	кінцева мережна служба (HTTP, Telnet тощо)	символьний
4	flag	статус з'єднання (нормальний чи помилковий)	символьний
5	src_byte	кількість байтів, переданих із передавача до приймача	числовий
6	dst_byte	кількість байтів, переданих із приймача до передавача	числовий
7	land	рівність хостів/портів приймача та передавача	символьний
8	wrong_fragment	кількість «неправильних» фрагментів	числовий
9	hot	кількість hot-індикаторів	числовий
10	num_failed_logins	кількість невдалих спроб логіна	числовий
…	…	…	…
41	dst_host_srv_rerror_rate	відсоток з'єднань із помилкою REJ для клієнтського сервісу	числовий

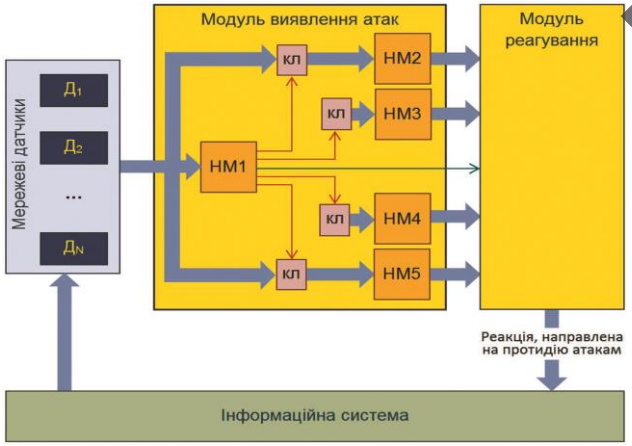


Рис. 1. Структура гіпотетичного комплексу

doi: https://doi.org/10.15802/stp2020/218318

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)
Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)

Нейромережа для виявлення категорії класу атаки або визначення факту її відсутності. Вхідний вектор складає 41 параметр TCP-з'єднання, вихідним є вектор із п'яти значень, чотири з яких представляють клас атаки, а п'ятий – штатне підключення. Це так званий one-hot vector – вектор, усі компоненти якого дорівнюють нулю, за винятком одного, який дорівнює одиниці. Цей компонент і буде вказувати на визначений нейронною мережею клас атаки або на звичайне підключення, якщо атаки не було. Кількість нейронів у прихованому шарі багатошарового персептрона можна визначити за відомою формулою, що є наслідком теореми Колмогорова–Арнольда–Хехт–Нільсена:

$$\frac{N_y Q}{1+log_2(Q)} \le N_w \le$$

$$\le N_y(\frac{Q}{N_x}+1)(N_x+N_y+1)+N_y, \quad (1)$$

де N_y – довжина вихідного сигналу; Q – число елементів множини навчальних прикладів; N_w – необхідна кількість синаптичних зв'язків; N_x – розмірність вхідного сигналу.

Оцінивши необхідну кількість синаптичних зв'язків, можна розрахувати необхідну кількість нейронів у прихованому шарі:

$$N = \frac{N_w}{N_x + N_y}. \quad (2)$$

Значення N_x, N_y, Q дорівнюють 41,5 та 1 024 записи відповідно. Знайдено, що $466 \le N_w \le 6110$; $11 \le N \le 132$. Візьмемо більше значення – 132 нейрони, тоді НМ1 буде мати конфігурацію 41–1–132–5, що представлена на рис. 2, де 41 – кількість вхідних нейронів, 1 – кількість прихованих шарів, 132 – кількість прихованих нейронів, 5 – кількість вихідних нейронів.

До речі, архітектури всіх інших НМ аналогічні та відрізняються лише кількістю нейронів у різних шарах, результати розрахунків зведені до табл. 2.

Загальна характеристика програмної моделі. Для створення програмної моделі використана мова програмування Python 3.5, інтегроване середовище розробки PyCharm 2016.3 та фреймворк Tensorflow 1.2 [12].

Програмний комплекс дозволяє будувати багатошаровий персептрон (додавати шари із заданою довжиною), тренувати й перевіряти нейронну модель. Окрім цього, можна виставляти такі параметри, як коефіцієнт сходження, кількість епох навчання, розмір порції даних для кроку навчання. За функцію оптимізації взято оптимізатор ADAM. У програмі можна розраховувати різницю відповідей нейромережі та еталонних мереж й отримувати значення точності.

Для аналізу нейронних моделей використано інструмент візуалізації Tensorboard.

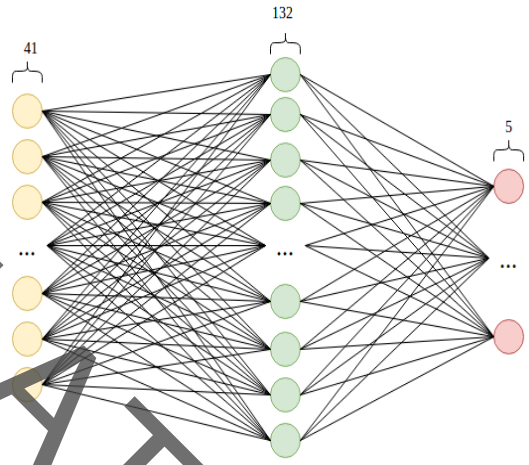


Рис. 2. НМ конфігурації 41–1–132–5 для виявлення категорії класу атаки

Результати

Як приклад наведено аналіз НМ1, яка визначає категорію класу атаки. Для НМ1 конфігурації 41–1–132–5 довжина навчальної, тестової та валідаційної вибірки становить 1 024, 294 та 156 прикладів відповідно.

Отримані графіки точності та похибки навчання НМ1 конфігурації 41–1–132–5 за ітераціями для різних швидкостей навчання представлено на рис. 3. Загальна кількість ітерацій навчання дорівнює 5 000; дані для навчання приходять по 100 рядків за ітерацію. Параметр Smoothing відповідає за апроксимацію кривих на графіках, що дозволяє оцінювати швидкість їх росту або спадання. Яскравими кольорами позначено апроксимовані графіки, блідими – їх істинний вигляд.

doi: https://doi.org/10.15802/stp2020/218318

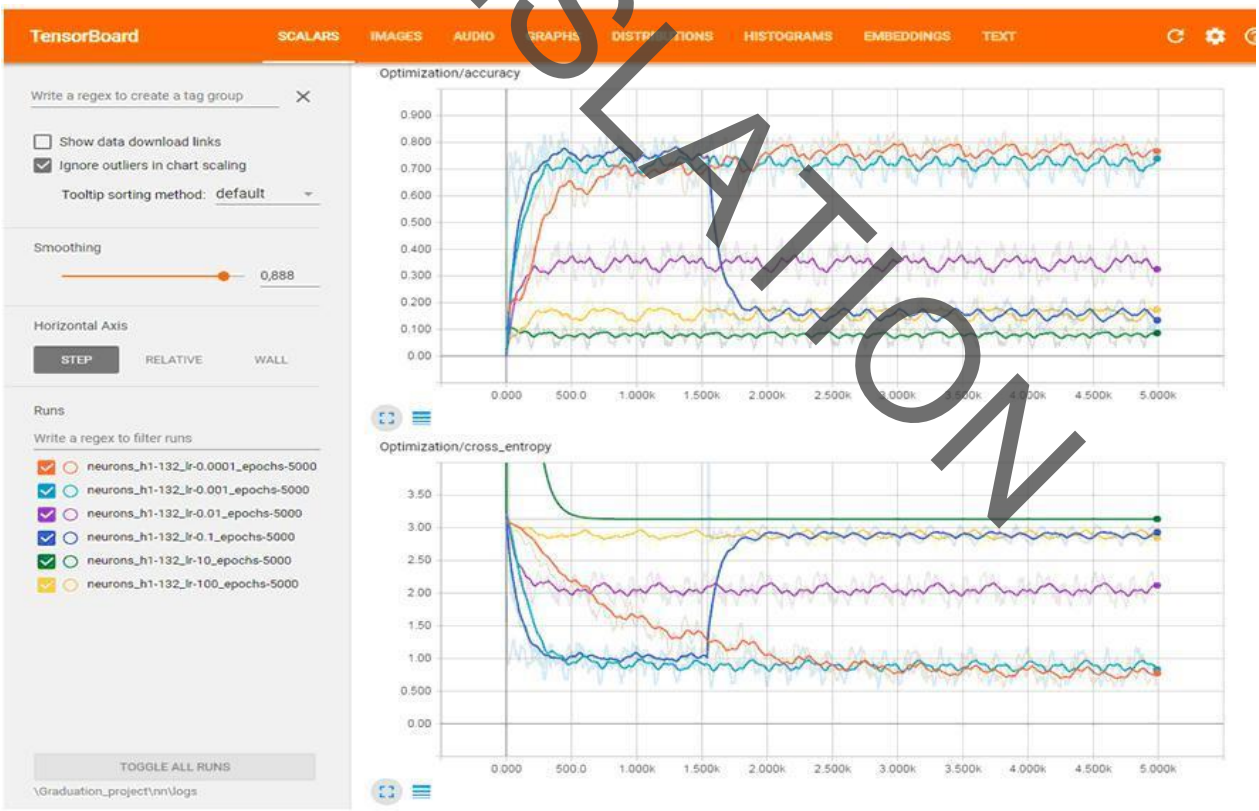
ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)

Таблиця 2

Параметри та конфігурація НМ

НМ	Призначення	Параметри НМ					Конфігурація
		N_x	N_y	Q	N_w	N	
НМ1	Виявлення категорії класу атаки	41	5	1 024	$466 \le N_w \le 6\,110$	$11 \le N \le 132$	41–1–132–5
НМ2	Виявлення типу атаки категорії DoS	41	7	1 024	$559 \le N_w \le 7\,487$	$12 \le N \le 160$	41–1–160–5
НМ3	Виявлення типу атаки категорії R2L	41	9	512	$410 \le N_w \le 5\,404$	$9 \le N \le 111$	41–1–111–5
НМ4	Виявлення типу атаки категорії U2R	41	5	32	$22 \le N_w \le 332$	$1 \le N \le 8$	41–1–8–5
НМ5	Виявлення типу атаки категорії Probe	41	5	1 024	$373 \le N_w \le 4\,787$	$9 \le N \le 107$	41–1–107–5



neurons_h1-N_lr-M_epochs-P:
N – кількість нейронів у прихованому шарі, *M* – швидкість навчання, *P* – кількість ітерацій навчання

Рис. 3. Точність і похибка навчання НМ 41–1–132–5 за ітераціями (для різних швидкостей навчання)

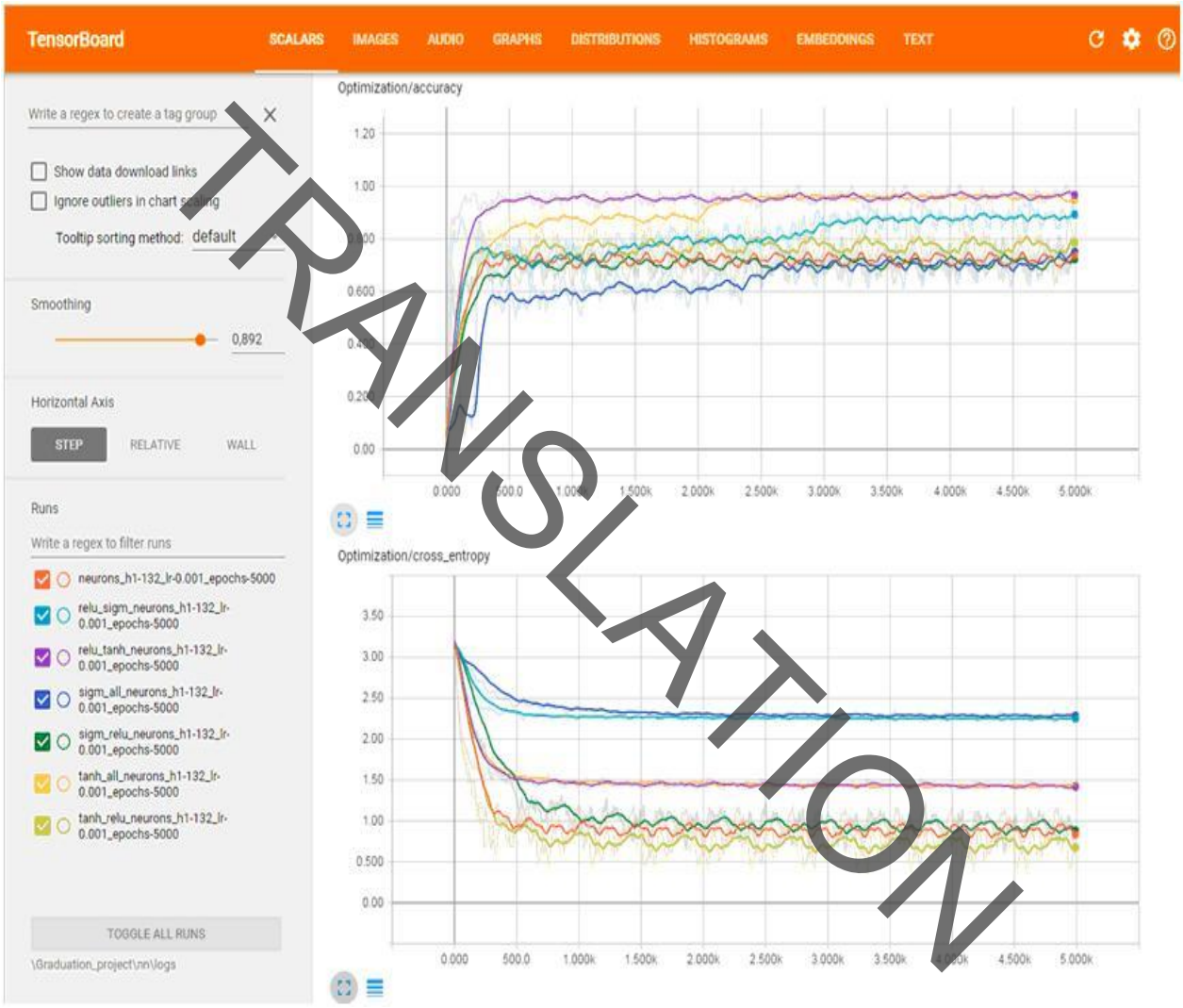
doi: https://doi.org/10.15802/stp2020/218318

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)

Як видно з рис. 3, за швидкості навчання 0,1 точність різко впала між другою та третьою тисячами ітерацій, що може бути наслідком поганої вибірки. Однак за швидкості навчання 0,0001 результат задовільний, а за швидкості навчання 0,001 – результат найкращий.

Одержані графіки точності та похибки навчання НМ1 конфігурації 41–1–132–5 за ітераціями для різних функцій активації представлені на рис. 4. Швидкість навчання при цьому дорівнює 0,001, кількість ітерацій навчання – 5 000, довжина порції даних на кожній ітерації – 100 рядків.



[f1_][f2_]neurons_h1-132_lr-0,001_epochs-5000:
*f*1, *f*2 – функції активації прихованого та вихідного шару; за замовченням – relu; all – *f*2 повторює *f*1

Рис. 4. Точність і похибка навчання НМ 41–1–132–5 за ітераціями (для різних функцій активації)

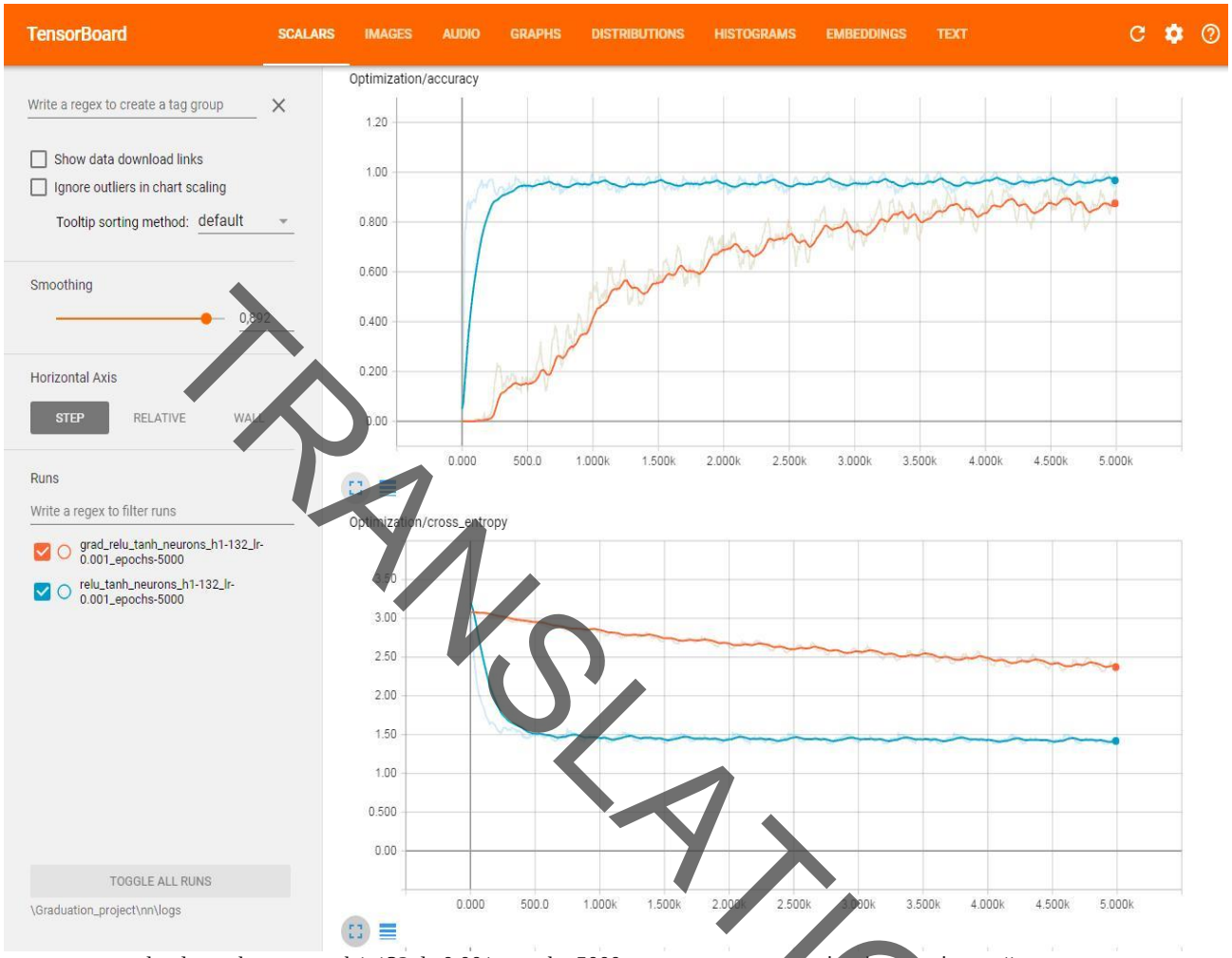
Із рис. 4 видно, що найкращі результати (витрачений час на навчання НМ менший) досягається в разі використання функції ReLU в прихованому шарі та гіперболічного тангенса у вихідному шарі.

Отримані графіки точності та похибки навчання НМ1 41–1–132–5 за ітераціями для різних алгоритмів оптимізації представлені на рис. 5. Параметри НМ1: швидкість навчання – 0,001, кількість ітерацій – 5 000, довжина порції даних – 100, функція активації прихованого шару – ReLU, функція активації вихідного шару – гіперболічний тангенс.

doi: https://doi.org/10.15802/stp2020/218318

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)



grad_relu_tanh_neurons_h1-132_lr-0,001_epochs-5000 – алгоритмом оптимізації є градієнтний спуск,
relu_tanh_neurons_h1-132_lr-0,001_epochs-5000 – алгоритмом оптимізації є ADAM

Рис. 5. Точність і похибка навчання НМ 41–1–132–5 за ітераціями (для різних алгоритмів оптимізації)

Із рис. 5 видно, що для НМ1 алгоритм ADAM працює швидше.

Визначено, що НМ1 конфігурації 41–1–132–5 надає найкраще значення точності за швидкості навчання 0,001 та потребує найменшого часу для навчання в разі використання напівлінійної функції активації ReLU в прихованому шарі та гіперболічного тангенса у вихідному шарі; алгоритм ADAM порівняно з алгоритмом градієнтного спуску працює швидше, дає більш високу точність та нижчу помилку. За результатами дослідження НМ1 конфігурації 41–1–132–5 для виявлення категорії класу атаки визначено параметри: швидкість навчання – 0,001; кількість ітерацій – 5 000; довжина порції даних – 100; функція активації в прихованому шарі – ReLU; функція активації у вихідному шарі – гіперболічний тангенс; алгоритм оптимізації – ADAM, за яких точність на тестовій та валідаційній вибірках склала 92,86 та 91,03 % відповідно.

Результати моделювання на інших нейронних мережах (точність визначення атаки) зведено до табл. 3.

doi: https://doi.org/10.15802/stp2020/218318

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)

Таблиця 3

Результати моделювання НМ

НМ	НМ1	НМ2	НМ3	НМ4	НМ5
Конфігурація	41–1–132–5	41–1–160–5	41–1–111–5	41–1–8–5	41–1–107–5
Точність, %	91,03	98,93	94,77	–	97,35

Із таблиці видно, що найкращий результат досягається під час визначення типу атак класів DoS та Probe, дещо гірше – для класу R2L. Для класу U2R налаштувати нейронну мережу НМ4 для отримання прийнятних результатів не вдалося. Це пояснюється малою кількістю записів (усього 52) в базі KDDCup99, які належать до класу U2R.

Наукова новизна та практична значимість

У нашій роботі виявлення мережних атак здійснено за допомогою застосування апарату нейронних мереж (багатошарового персептрона), як і в інших роботах [10, 13], що не є протиріччям до тих робіт [1, 4, 5], де використовано гібридний підхід (імунні механізми та SOM; нейронний, імунний та нейронечіткий класифікатори) чи комбінований на основі різних типів нейронних мереж (MLP та нейронечітка мережа; декілька SOM та нейронечітка мережа; MLP, RBF та SOM). При цьому в нашій роботі досліджено всі типи атак класів DoS; U2R; R2L; Probe, а не окремі, як у роботах [10, 13].

Ми вважаємо, що використання багатошарового персептрона як математичного апарату є доцільним і достатнім. Наприклад, хоча мережа RBF і навчається швидше, ніж мережа MLP, але необхідно визначити кількість радіальних елементів, розташовування їх центрів і значення відхилення, модель RBF потребує дещо більшої кількості елементів, тобто буде працювати повільніше і потребує більше пам’яті, ніж модель MLP.

Обробка великого обсягу мережного трафіка, який постійно змінюється, на основі MLP з використанням машинного навчання (особливо глибокого) призводить до великої кількості помилкових спрацьовувань і пропусків атак, що потребує додаткових досліджень за використання технології DataMining [8]. Так, зокрема, у нашій роботі на програмній моделі визначено, що алгоритм оптимізації ADAM порівняно з алгоритмом градієнтного спуску працює швидше, дає більш високу точність та нижчу помилку; це не може бути протиріччям до використання інших засобів (зокрема, локального адаптивного багатофакторного згладжування, запропонованого у [7]).

У дослідженні використано багаторівневий (а саме дворівневий) підхід до побудови мережної системи виявлення вторгнень у комп’ютерну мережу: визначення категорії класу атаки (перший рівень); віднесення типу атаки до відповідного класу (другий рівень), що також не є протиріччям до модульного підходу у [2]. Але ймовірність помилки II роду (кількість пропусків атак) у нашій роботі складає приблизно 10 проти 18 % за модульним підходом, який реалізований у [2], що краще в 1,8 раза.

Висновки

1. Під час обробки великого обсягу мережного трафіка, який постійно змінюється, доречно застосовувати дворівневу мережну систему, основу якої складають п’ять нейронних мереж таких конфігурацій: 41–1–132–5 для визначення категорії класу атаки на першому рівні, а також 41–1–160–7, 41–1–8–5, 41–1–111–9, 41–1–107–5 для виявлення типу атаки із класів DoS (back, land, neptune, pod, smurf, teardrop), U2R (buffer_overflow, loadmodule, perl, rootkit), R2L (ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster), Probe (ipsweep, nmap, portsweep, satan) відповідно на другому рівні. Дані для навчання взято з відкритої бази даних KDDCup99, у якій зберігається велика кількість характеристик TCP-з’єднань. Для побудови всіх нейронних мереж обрано фреймворк для машинного навчання Google TensorFlow через його гнучкість та швидкість роботи.

2. Проведено дослідження параметрів нейронної мережі конфігурації 41–1–132–5, яка визначає категорію класу атаки на комп’ютерну мережу. Визначено, що оптимальна швидкість навчання дорівнює 0,001. Для оптимізації най-

doi: https://doi.org/10.15802/stp2020/218318

краще себе показав алгоритм ADAM. Як функція активації для прихованого шару найбільше підходить функція ReLU, для функції активації вихідного шару – функція гіперболічного тангенса. Точність на тестовій та валідаційній вибірках склала 92,86 та 91,03 % відповідно. Імовірність помилки II роду складає приблизно 10 %.

3. Дослідження показало, що для навчання нейронної мережі конфігурації 41–1–8–5, що визначає тип атаки класу U2R, доступної навчальної вибірки недостатньо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Браницкий А. А. Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта : автореф. дис. ... канд. техн. наук. Санкт-Петербург, 2018. 18 с.
2. Жульков Е. В. Построение модульных нейронных сетей для обнаружения классов сетевых атак : автореф. дис. ... канд. техн. наук. Санкт-Петербург, 2007. 16 с.
3. Пахомова В. М., Конпов М. С. Дослідження двох підходів до виявлення мережних атак із використанням нейромережної технології. Наука та прогрес транспорту. 2020. № 3 (87). С. 81–93. DOI: https://doi.org/10.15802/stp2020/208233
4. Фролов П. В., Чухраев И. В., Гришанов К. М. Применение искусственных нейронных сетей в системах обнаружения вторжений. Системный администратор. 2018. № 9 (190). URL: http://samag.ru/archive/article/3724 (дата звернення: 04.09.2020).
5. Amini M., Rezaeenour J., Hadavandi E. A Neural Network Ensemble Classifier for Effective Intrusion Detection using Fuzzy Clustering and Radial Basis Function Networks. International Journal on Artificial Intelligence Tools. 2016. Vol. 25. Iss. 02. P. 1–32. DOI: https://doi.org/10.1142/s0218213015500335
6. Esteban J. A New GHSOM Model applied to network security. Artificial Neural Networks-ICANN 2008. 2008. P. 680–689.
7. Grill M., Pevný T., Rehak M. Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. *Journal of Computer and System Sciences*. 2017. Vol. 83. Iss. 1. P. 43–57. DOI: https://doi.org/10.1016/j.jcss.2016.03.007
8. Hadi, A. A. A. Performance Analysis of Big Data Intrusion Detection System over Random Forest Algorithm. International Journal of Applied Engineering Research. 2018. Vol. 13, No. 2. P. 1520–1527.
9. KDD Cup 1999 Data. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (дата звернення: 04.09.2020).
10. Saied A., Overill R. E., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing. 2016. Vol. 172. P. 385–393. DOI: https://doi.org/10.1016/j.neucom.2015.04.101
11. Sikos L. F. AI in Cybersecurity. New York : Springer, 2018. 205 p.
12. TensorFlow. URL: http://www.tensorflow.org (дата звернення: 04.09.2020).
13. Zhukovyts'kyy I. V., Pakhomova V. M. Identifying threats in computer network based on multilayer neural network. Наука та прогрес транспорту. 2018. № 2 (74). P. 114–123. DOI: https://doi.org/10.15802/stp2018/130797
14. 2018 Data Breach Investigations Report. URL: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf (дата звернення: 04.09.2020).

И. В. ЖУКОВИЦКИЙ[1*], В. Н. ПАХОМОВА[2*], Д. А. ОСТАПЕЦ[3*], О. И. ЦЫГАНОК[4*]

[1*] Каф. «Электронные вычислительные машины», Днипровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днипро, Украина, 49010, тел. +38 (056) 373 15 89, эл. почта ivzhukl@ua.fm, ORCID 0000-0002-3491-5976

[2*] Каф. «Электронные вычислительные машины», Днипровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днипро, Украина, 49010, тел. +38 (056) 373 15 89, эл. почта viknikpakh@gmail.com, ORCID 0000-0002-0022-099X

[3*] Каф. «Электронные вычислительные машины», Днипровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днипро, Украина, 49010, тел. +38 (056) 373 15 89, эл. почта odaua@i.ua, ORCID 0000-0003-1778-7770

[4*] Каф. «Электронные вычислительные машины», Днипровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днипро, Украина, 49010, тел. +38 (056) 373 15 89, эл. почта tsiganok.oleg@yandex.ua, ORCID 0000-0001-9846-7669

doi: https://doi.org/10.15802/stp2020/218318

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 5 (89)

ОБНАРУЖЕНИЕ АТАК НА КОМПЬЮТЕРНУЮ СЕТЬ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ КОМПЛЕКСА НЕЙРОННЫХ СЕТЕЙ

Цель. В качестве основной цели исследования поставлено развитие методики определения атак на компьютерную сеть. Достижение поставленной цели предусматривает решение следующих задач: разработать методику выявления атак на компьютерную сеть на основе ансамбля нейронных сетей с использованием нормализованных данных открытой базы KDDCup99; при выполнении машинного обучения выявить оптимальные параметры нейронной сети, что обеспечит достаточно высокий уровень достоверности обнаружения вторжений в компьютерную сеть. **Методика.** В качестве архитектурного решения модуля обнаружения атак предложено двухуровневую сетевую систему, основу которой составляет ансамбль из пяти нейронных сетей типа многослойного персептрона: первая нейронная сеть – для определения категории класса атаки (DoS, R2L, U2R, Probe) или факта того, что атаки не было; другие нейронные сети – для выявления типа атаки, если таковая имела место (каждая из этих четырех нейронных сетей соответствует одному классу атаки и умеет определять типы, принадлежащих только этому классу). **Результаты.** На созданной программной модели проведено исследование параметров нейронной сети конфигурации 41–1–132–5, которая определяет категорию класса атаки на компьютерную сеть. Установлено, что оптимальная скорость обучения равна 0,001. Для оптимизации лучше всего себя показал алгоритм ADAM. В качестве функции активации для скрытого слоя более всего подходит функция ReLU, для функции активации выходного слоя – функция гиперболического тангенса. Точность на тестовой и валидационной выборках составила 92,86 и 91,03 % соответственно. **Научная новизна.** Разработанная программная модель, для которой использован язык программирования Python 3.5, интегрированная среда разработки PyCharm 2016.3 и фреймворк Tensorflow 1.2, дает возможность обнаруживать все типы атак классов DoS, U2R, R2L, Probe. **Практическая значимость.** Получены графические зависимости точности нейронных сетей при различных параметрах: скорости обучения; активационной функции; алгоритма оптимизации. Определены оптимальные параметры нейронных сетей, которые обеспечат достаточно высокий уровень достоверности обнаружения вторжений в компьютерную сеть.

Ключевые слова: архитектурное решение; нейронная сеть; скорость обучения; функция активации; алгоритм оптимизации

I. V. ZHUKOVYTS'KYY[1*], V. M. PAKHOMOVA[2*], D. O. OSTAPETS[3*], O. I. TSYHANOK[4*]

[1*]Dep. «Electronic Computing Machines», Dnipro National University of Railway Transport named after Academician V. Lazaryan, Lazaryana St., 2, Dnipro, Ukraine, 49010, tel. +38 (056) 373 15 89, e-mail ivzhukl@ua.fm, ORCID 0000-0002-3491-5976
[2*]Dep. «Electronic Computing Machines», Dnipro National University of Railway Transport named after Academician V. Lazaryan, Lazaryana St., 2, Dnipro, Ukraine, 49010, tel. +38 (056) 373 15 89, e-mail viknikpakh@gmail.com, ORCID 0000-0002-0022-099X
[3*]Dep. «Electronic Computing Machines», Dnipro National University of Railway Transport named after Academician V. Lazaryan, Lazaryana St., 2, Dnipro, Ukraine, 49010, tel. +38 (056) 373 15 89, e-mail odaua@i.ua, ORCID 0000-0003-1778-7770
[4*]Dep. «Electronic Computing Machines», Dnipro National University of Railway Transport named after Academician V. Lazaryan, Lazaryana St., 2, Dnipro, Ukraine, 49010, tel. +38 (056) 373 15 89, e-mail tsiganok.oleg@yandex.ua, ORCID 0000-0001-9846-7669

DETECTION OF ATTACKS ON A COMPUTER NETWORK BASED ON THE USE OF NEURAL NETWORKS COMPLEX

Purpose. The article is aimed at the development of a methodology for detecting attacks on a computer network. To achieve this goal the following tasks were solved: to develop a methodology for detecting attacks on a computer network based on an ensemble of neural networks using normalized data from the open KDD Cup 99 database; when performing machine training to identify the optimal parameters of the neural network which will provide a sufficiently high level of reliability of detection of intrusions into the computer network. **Methodology.** As an architectural solution of the attack detection module, a two-level network system is proposed, based on an ensemble of five neural networks of the multilayer perceptron type. The first neural network to determine the category of attack class (DoS, R2L, U2R, Probe) or the fact that there was no attack; other neural networks – to detect the type of at-

doi: https://doi.org/10.15802/stp2020/218318

tack, if any (each of these four neural networks corresponds to one class of attack and is able to identify types that belong only to this class). **Findings.** The created software model was used to study the parameters of the neural network configuration 41–1–132–5, which determines the category of the attack class on the computer network. It is determined that the optimal training speed is 0.001. The ADAM algorithm proved to be the best for optimization. The ReLU function is the most suitable activation function for the hidden layer, and the hyperbolic tangent function – for the output layer activation function. Accuracy in test and validation samples was 92.86 % and 91.03 %, respectively. **Originality.** The developed software model, which uses the Python 3.5 programming language, the integrated development environment PyCharm 2016.3 and the Tensorflow 1.2 framework, makes it possible to detect all types of attacks of DoS, U2R, R2L, Probe classes. **Practical value.** Graphical dependencies of accuracy of neural networks at various parameters are received: speed of training; activation function; optimization algorithm. The optimal parameters of neural networks have been determined, which will ensure a sufficiently high level of reliability of intrusion detection into a computer network.

Keywords: architectural solution; neural network; training speed; activation function; optimization algorithm

REFERENCES

1. Branitskiy, A. A. (2018). *Obnaruzhenie anomalnykh setevykh soedineniy na osnove gibridizatsii metodov vychislitelnogo intellekta* (Extended abstract of PhD dissertation). St. Petersburg, Russia. (in Russian)
2. Zhulkov, Ye. V. (2007). *Postroenie modulnykh neyronnykh setey dlya obnaruzheniya klassov setevykh atak* (Extended abstract of PhD dissertation). St. Petersburg, Russia. (in Russian)
3. Pakhomova, V. M., & Konnov, M. S. (2020). Research of two approaches to detect network attacks using neural network technologies. *Science and Transport Progress, 3*(87), 81-93. DOI: https://doi.org/10.15802/stp2020/208233 (in Ukrainian)
4. Frolov, P. V., Chukhraev, I. V., & Grishanov, K. M. (2018). Application of artificial neural networks in intrusion detection systems. *System administrator, 9*(190). Retrieved from samag.ru/archve/article/3724 (in Russian)
5. Amini, M., Rezaeenour, J., & Hadavandi, E. (2016). A Neural Network Ensemble Classifier for Effective Intrusion Detection Using Fuzzy Clustering and Radial Basis Function Networks. *International Journal on Artificial Intelligence Tools, 25*(02), 1-32. DOI: https://doi.org/10.1142/s0218213015500335 (in English)
6. Esteban, J. (2008). A New GHSOM Model applied to network security. *Artificial Neural Networks-ICANN 2008* (pp. 680-689). (in English)
7. Grill, M., Pevný, T., & Rehak, M. (2017). Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. *Journal of Computer and System Sciences, 83*(1), 43-57. DOI: https://doi.org/10.1016/j.jcss.2016.03.007 (in English)
8. Hadi, A. A. A. (2018). Performance Analysis of Big Data Intrusion Detection System over Random Forest Algorithm. *International Journal of Applied Engineering Research, 13*(2), 1520-1527 (in English)
9. KDD Cup 1999 Data. Retrieved from http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (in English)
10. Saied, A., Overill, R. E., & Radzik, T. (2016). Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing, 172*, 385-393. DOI: https://doi.org/10.1016/j.neucom.2015.04.101 (in English)
11. Sikos, L. F. (2018). *AI in Cybersecurity*. New York: Springer. (in English)
12. TensorFlow. Retrieved from http://www.tensorflow.org (in English)
13. Zhukovyts'kyy, I. V., & Pakhomova, V. M. (2018). Identifying threats in computer network based on multilayer neural network. *Science and Transport Progress, 2*(74), 114-123. DOI: https://doi.org/10.15802/stp2018/130797 (in English)
14. 2018 Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf (in English)

Надійшла до редколегії: 28.05.2020
Прийнята до друку: 28.09.2020

doi: https://doi.org/10.15802/stp2020/218318