УДК 004.056.53:[004.7:004.032.26]
DOI https://doi.org/10.32782/2663-5941/2023.4/15

***Пахомова В.М.***
Український державний університет науки і технологій

***Квочка М.Ю.***
Український державний університет науки і технологій

# ВИЗНАЧЕННЯ МЕРЕЖЕВИХ АТАК КАТЕГОРІЇ PROBE ЗАСОБАМИ БАГАТОШАРОВОЇ НЕЙРОННОЇ МЕРЕЖІ

*Для виявлення мережевих атак в режимі реального часу використовуються системи визначення вторгнень (Intrusion Detection System, IDS), в яких з'являється проблема великого обсягу мережевого трафіку і для вирішення якої доцільно використання нейромережної технології, що підтверджує актуальність теми. В роботі проведено дослідження наступних мережевих атак категорії PROBE: Ipsweep; Nmap; Portsweep; Satan з використанням відкритої бази даних NSL-KDD засобами нейронної мережі конфігурації 41-1-X-5, що створена в середовищі MatLAB за допомогою додатку Toolbox, а також визначення її оптимальних параметрів та оцінювання параметрів якості виявлення мережевих атак категорії PROBE на створеній нейронній мережі. Проведено дослідження середньоквадратичної похибки створеної нейронної мережі при різній кількості прихованих нейронів (20, 40, 60 та 80) за різними алгоритмами навчання (Levenberg-Marquardt, Bayesian regularization та Scaled Conjugate Gradient) на вибірках різної довжини (250, 750 та 1500 прикладів). Визначено, що найменше значення похибки створеної нейронної мережі досягнуто при 60 прихованих нейронів за алгоритмом навчання Levenberg-Marquardt на вибірці із 1500 прикладів. Виконано оцінювання параметрів якості виявлення мережевих атак категорії PROBE на створеній нейронній мережі. Визначено, що значення помилки першого та другого роду склали 6,67 % та 5,33 % відповідно.*

***Ключові слова:*** *атака, мережевий клас, PROBE, прихований нейрон, довжина вибірки, алгоритм навчання, похибка, оцінка якості.*

**Постановка проблеми.** Створення ефективної системи виявлення мережевих атак вимагає застосування якісно нових підходів до обробки інформації, які повинні ґрунтуватися на адаптивних алгоритмах здатних до самонавчання. Найбільш перспективним напрямком у створенні подібних систем виявлення мережевих атак є застосування нейромережної технології.

**Аналіз останніх досліджень і публікацій.** Відомо, що для виявлення мережевих атак доцільно використання нейромережної технології [2–10, 12], зокрема багатошарового персептрону (Multi Layer Perceptron, MLP) [2, 12], самоорганізуючої карти Кохонена (Self Organizing Map, SOM) [3, 9], радіально-базисної мережі (Radial Basis Function Network, RBF) [5, 7], а також нейронечіткої мережі (Adaptive-Network-Based Fuzzy Inference System, ANFIS) [4, 7]. На сьогодні відомо, що різні НМ, в основі яких різні математичні апарати, можуть по різному визначати різні атаки на комп'ютерну мережу. Однак, разом з тим важливим недоліком таких методик є відсутність універсальності їх застосування при визначенні мережевих атак різних категорій: DoS; PROBE; R2L; U2R, серед яких найбільша кількість досліджень стосовно категорії DoS [5–6]. Для виявлення мережевих атак категорії PROBE авторами був використаний SOM в [3] та нейронечітка мережа в [4], але відомо, що властивості MLP дозволяють його також використати для виявлення мережевих атак цієї категорії, однак це потребує проведення додаткового дослідження стосовно оптимальних параметрів MLP (кількості прихованих нейронів, довжини вибірки та алгоритму навчання).

**Формулювання цілей статті.** Проведені дослідження ставили за мету розвиток методики виявлення мережевих атак категорії PROBE. Для досягнення поставленої мети вирішувалися наступні задачі: розробити методику виявлення мережевих атак засобами багатошарової нейронної мережі (НМ); при виконанні машинного навчанні виявити оптимальні параметри НМ, що забезпечить достатньо високий рівень достовірності виявлення вторгнень в комп'ютерну мережу; оцінити помилки першого та другого роду при виявленні мережевих атак на створеній НМ.

**Виклад основного матеріалу дослідження.** Мережева категорія PROBE представляє одну

з чотирьох категорій атак, що спрямована на сканування портів з метою отримання конфіденційної інформації. Основні мережеві класи атак категорії PROBE: Ipsweep (атака полягає у скануванні мережевого простору з метою виявлення активних хостів); Nmap (атака використовується для сканування портів хостів з метою виявлення відкритих портів та отримання інформації про сервіси, які запущені на цих портах); Portsweep (атака полягає у скануванні портів на окремому хості з метою виявлення відкритих портів та отримання інформації про сервіси, які запущені на цих портах); Satan (збір детальної інформації про систему та виявлення вразливостей, які можна використати для злому). У якості початкових даних використана відкрита база даних NSL-KDD [11]. У якості методу дослідження використано MLP, структура якого подана на рис. 1.

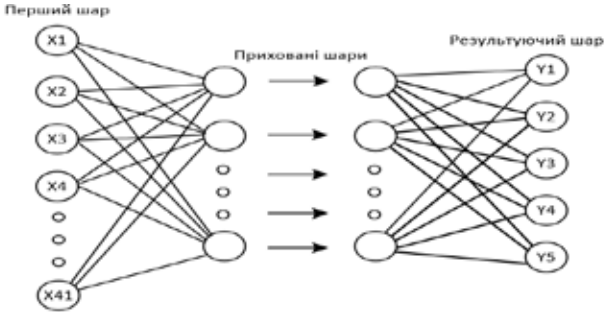


**Рис. 1. Структура багатошарового персептрону**

Перший шар НМ має X1…X41 нейрони (це параметри мережевого трафіку), що зведені до таблиці 1. Результуючий шар має наступні нейрони: Y1 – Normal (нормальний стан: відсутність атаки на комп'ютерну мережу); Y2 – атака класу Nmap; Y3 – атака класу Satan; Y4 – атака класу Ipsweep; Y5 – атака класу Portsweep.

Таблиця 1

**Перелік нейронів першого шару НМ**

| Нейрон | Назва | Опис |
|---|---|---|
| X1 | duration | тривалість з'єднання |
| X2 | protocol_type | тип протоколу |
| X3 | service | сервіс, який використовується в з'єднанні |
| X4 | flag | прапорець, що вказує статус пакета |
| X5 | src_bytes | кількість байтів відправлених від джерела до призначення |
| X6 | dst_bytes | кількість байтів відправлених від призначення до3 джерела |
| X7 | land | вказує, чи є з'єднання land-атакою (1 – так, 0 – ні) |
| X8 | wrong_fragment | кількість неправильних фрагментів |
| X9 | urgent | кількість, пакетів з високим пріоритетом |
| X10 | hot | кількість «гарячих» (часто відвідуваних) пунктів призначення |
| X11 | num_failed_logins | кількість неуспішних спроб входу |
| X12 | logged_in | прапорець, що показує, чи було виконано вхід в систему |
| X13 | num_compromised | кількість компрометованих систем, пов'язаних з пакетом |
| X14 | root_shell | вказує, чи було встановлено root shell |
| X15 | su_attempted | прапорець, що показує, чи була спроба використання команди підняття привілеїв |
| X16 | num_root | кількість команд від root |
| X17 | num_file_creations | кількість створених файлів |
| X18 | num_shells | кількість оболонок, виконаних під час сеансу |
| X19 | num_access_files | кількість файлів з доступом |
| X20 | num_outbound_cmds | кількість вихідних команд |
| X21 | is_host_login | прапорець, що показує, чи було виконано вхід як хост |
| X22 | is_guest_login | прапорець, що показує, чи було виконано вхід як гість |
| X23 | count | кількість з'єднань до хоста за останню секунду |
| X24 | srv_count | кількість з'єднань до одного сервісу за останню секунду |
| X25 | serror_rate | частота з'єднань з помилками (сервісні помилки) |
| X26 | srv_serror_rate | частота з'єднань до одного сервісу з помилками (сервісні помилки) |
| X27 | rerror_rate | частота з'єднань з помилками (системні помилки) |
| X28 | srv_rerror_rate | частота з'єднань до одного сервісу з помилками (системні помилки) |
| X29 | same_srv_rate | частота з'єднань до одного сервісу з однаковим типом сервісу |
| X30 | diff_srv_rate | частота з'єднань до різних сервісів |

Продовження таблиці 1

| Нейрон | Назва | Опис |
|---|---|---|
| X31 | srv_diff_host_rate | частота з'єднань до різних хостів для одного сервісу |
| X32 | dst_host_count | кількість унікальних хостів, на які відбулися зєднання |
| X33 | dst_host_srv_count | кількість унікальних хостів, на які відбулися зєднання до одного сервісу |
| X34 | dst_host_same_srv_rate | частота зєднань до одного сервісу на одному хості |
| X35 | dst_host_diff_srv_rate | частота з'єднань до різних сервісів на одному хості |
| X36 | dst_host_same_src_port_rate | частота з'єднань з одного порту джерела до одного порту призначення, |
| X37 | dst_host_srv_diff_host_rate | частота з'єднань до різних хостів для одного сервісу на одному хості |
| X38 | dst_host_serror_rate | частота з'єднань до одного хосту з помилками (сервісні помилки) |
| X39 | dst_host_srv_serror_rate | частота з'єднань до одного сервісу на одному хосту з помилками (сервісні помилки) |
| X40 | dst_host_rerror_rate | частота з'єднань до одного хосту з помилками (системні помилки) |
| X41 | dst_host_srv_rerror_rate | частота з'єднань до одного сервісу на одному хосту з помилками (системні помилки) |

Таблиця 2

**Фрагмент вибірки (для нейронів першого шару)**

| X1 | X2 | X3 | X4 | X5 | X6 | X7 | X8 | X9 | X10 | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 2 | 1 | 1 | 8 | 0 | 0 | 0 | 0 | 0 | |
| 0 | 1 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 0 | 2 | 1 | 1 | 8 | 0 | 0 | 0 | 0 | 0 | |
| **X11** | **X12** | **X13** | **X14** | **X15** | **X16** | **X17** | **X18** | **X19** | **X20** | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| **X21** | **X22** | **X23** | **X24** | **X25** | **X26** | **X27** | **X28** | **X29** | **X30** | |
| 0 | 0 | 1 | 26 | 0 | 0 | 0 | 0 | 1 | 0 | |
| 0 | 0 | 365 | 1 | 0,1 | 0 | 0,9 | 1 | 0 | 1 | |
| 0 | 0 | 1 | 41 | 0 | 0 | 0 | 0 | 1 | 0 | |
| **X31** | **X32** | **X33** | **X34** | **X35** | **X36** | **X37** | **X38** | **X39** | **X40** | **X41** |
| 1 | 3 | 115 | 1 | 0 | 1 | 0,3 | 0 | 0 | 0 | 0 |
| 0 | 255 | 1 | 0 | 1 | 0 | 0 | 0,1 | 0 | 0,9 | 1 |
| 1 | 2 | 106 | 1 | 0 | 1 | 0,5 | 0 | 0 | 0 | 0 |

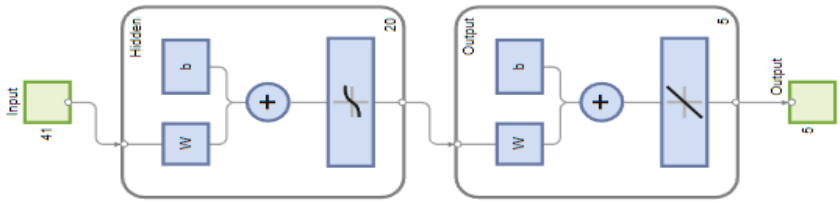


**Рис. 2. Структура створеної НМ в MatLAB**

***Формування вибірки***. На основі відкритої бази даних NSL-KDD складено вибірку із 250 прикладів (по 50 прикладів на кожний мережевий клас), фрагмент якої представлено в таблиці 2 у якості прикладу.

***Створення НМ.*** За допомогою пакета Toolbox в MatLAB створено НМ конфігурації 41-1-20-5 [1], де 41 – кількість нейронів першого шару (параметри мережевого трафіку), 1 – кількість прихованих шарів, 20 – кількість прихованих нейронів, 5 – кількість результуючих нейронів; у якості функції активації прихованого шару взято гіперболічний тангенс, на результуючому шарі – лінійна функція. Створено в MatLAB НМ, структуру якої відображено на рис. 2; отримані результати

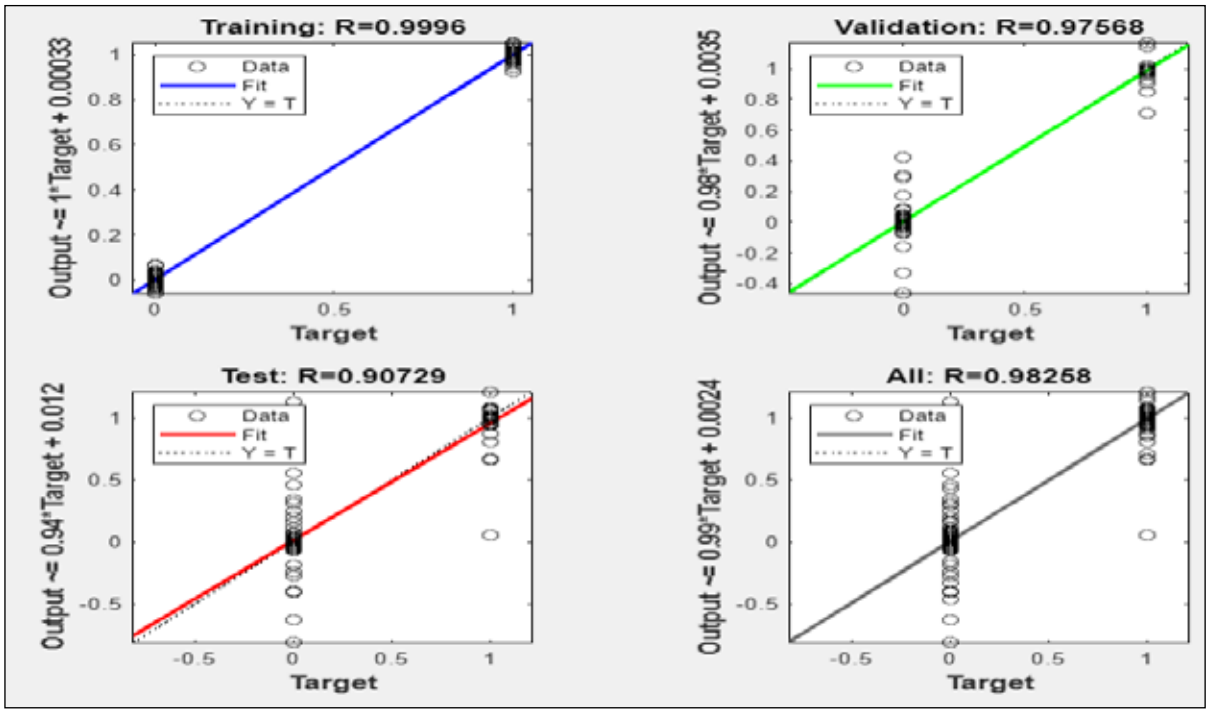


**Рис. 3. Отримані результати на НМ конфігурації 41-1-20-5**

(значення регресії) на створеній НМ показано на рис. 3.

***Визначення оптимальних параметрів НМ.*** На створеній НМ проведено дослідження похибки (Mean Square Error, MSE) при різній кількості прихованих нейронів (20, 40, 60 та 80) за наступними алгоритмами навчання НМ: Levenberg-Marquardt; Bayesian regularization; Scaled Conjugate Gradient) на вибірках різної довжини (250, 750 та 1500 прикладів). Визначено, що найменше значення похибки НМ склало 0,0071 при 60 прихованих нейронів за алгоритмом навчання Levenberg-Marquardt на вибірці із 1500 прикладів (по 300 прикладів на кожний мережевий клас).

***Оцінка параметрів якості.*** На створеній НМ конфігурації 41-1-60-5 при визначених оптимальних параметрах отримані наступні результати: TP (True Positive); FP (False Positive); FN (False Negative); TN (True Negative).

Помилка першого роду – це кількість невірно виявлених атак (FP, False Positive), а помилка другого роду – це кількість пропусків атак (FN, False Negative); обчислені значення помилок першого та другого роду відповідно до мережевого класу атак категорії PROBE зведені до таблиці 4.

Із таблиці 4 видно, що на створеній НМ найкраще визначаються атаки мережевих класів Ipsweep та Portsweep.

Таблиця 3

**Отримані значення похибки НМ конфігурації 41-1-X-5**

| Кількість прихованих нейронів | Кількість прикладів | Алгоритм навчання | MSE |
|---|---|---|---|
| 20 | 250 | Levenberg-Marquardt | 0,0312 |
| 20 | 750 | Levenberg-Marquardt | 0,0262 |
| 20 | 1500 | Levenberg-Marquardt | 0,0114 |
| 40 | 1500 | Levenberg-Marquardt | 0,0074 |
| 60 | 1500 | Levenberg-Marquardt | 0,0071 |
| 80 | 1500 | Levenberg-Marquardt | 0,0158 |
| 60 | 1500 | Bayesian regularization | 0,0277 |
| 60 | 1500 | Scaled Conjugate Gradient | 0,0172 |

Таблиця 4

**Помилка першого та другого роду на НМ конфігурації 41-1-60-5**

| Мережевий клас атаки | Кількість неправильно виявлених атак | Кількість пропусків атак |
|---|---|---|
| Normal | 30 з 300 | 30 з 300 |
| Nmap | 30 з 300 | 30 з 300 |
| Satan | 40 з 300 | 20 з 300 |
| Ipsweep | 0 з 300 | 0 з 300 |
| Portsweep | 0 з 300 | 0 з 300 |
| Усього: | 100 з 1500 | 80 з 1500 |

Крім того, проведено розрахунок деяких інших параметрів якості. TPR (True Positive Rate) пред-

ставляє відношення правильно виявлених позитивних екземплярів (TP) до загальної кількості позитивних екземплярів (TP + FN). FPR (False Positive Rate) визначається як відношення кількості неправильно виявлених позитивних екземплярів (FP) до загальної кількості негативних екземплярів (FP + TN). Accuracy визначається як відношення загальної кількості правильно класифікованих екземплярів (TP + TN) до загальної кількості екземплярів (TP + TN + FP + FN). Precision визначається як відношення кількості правильно виявлених позитивних екземплярів (TP) до загальної кількості позитивно виявлених екземплярів (TP + FP). Recall визначається як відношення кількості правильно виявлених позитивних екземплярів (TP) до загальної кількості позитивних екземплярів (TP + FN). Обчислені значення параметрів якості зведені до таблиці 5.

Таблиця 5

**Показники оцінки якості виявлення атак на НМ конфігурації 41-1-60-5**

| TP | FP | FN | TN | TPR | FPR | Accuracy | Precision | Recall |
|---|---|---|---|---|---|---|---|---|
| 1300 | 100 | 80 | 20 | 0,94 | 0,83 | 0,9 | 0,93 | 0,94 |

Із таблиці 5 видно, що при виявленні мережевих атак категорії PROBE на створеній НМ значення помилки першого та другого роду склали 6,67 % та 5,33 % відповідно.

***Практична значимість.*** У [3] найменшу точність показала самоорганізуюча карта Кохонена при виявленні атак мережевого класу Nmap; одночасне використання створеної нейронної мережі, а також нейронечіткої мережі для визначення ступеню здійснення атаки категорії PROBE [4] та самоорганізуючої карти Кохонена для виявлення мережевого класу категорії PROBE [3] дозволить підвищити точність виявлення атак цього класу при використанні комбінованого варіанту.

**Висновки.** Для виявлення наступних мережевих класів атак категорії PROBE: Nmap; Satan; Portsweep; Ipsweep запропоновано нейронну мережу конфігурації 41-1-X-5, де 41 – кількість нейронів першого шару (параметри мережевого трафіку); 1 – кількість прихованих шарів; X – кількість прихованих нейронів; 5 – кількість результуючих нейронів (1 – наявність втвки, 0 – її відсутність). В системі MatLAB за допомогою додатку Toolbox створено нейронну мережу конфігурації 41-1-20-5, у якості функції активації нейронів на прихованому шарі якої взято гіперболічний тангенс, на результуючому шарі - лінійну функцію. Визначено, що значення похибки нейронної мережі склало приблизно 0,03 за алгоритмом навчання Levenberg-Marquardt на вибірці із 250 прикладів (по 50 прикладів на кожний мережевий клас категорії PROBE). На створеній нейронній мережі проведено дослідження похибки при різній кількості прихованих нейронів (20, 40, 60 та 80) за різними алгоритмами навчання (Levenberg-Marquardt, Bayesian regularization та Scaled Conjugate Gradient) на вибірках різної довжини (250, 750 та 1500 прикладів). Визначені оптимальні параметри створеної нейронної мережі, на якій виконано оцінювання якості виявлення мережевих атак категорії PROBE: помилка першого роду склала 6,67 %, а помилка другого роду – 5,33 %. На створеній нейронній мережі найкраще визначаються атаки мережевих класів Ipsweep та Portsweep.

**Список літератури:**

1. Квочка М. Ю. Виявлення мережевих атак категорії PROBE з використанням нейромережної технології : дипломна робота на здобуття кваліфікаційного ступеня бакалавра : спец. 125 – кібербезпека / наук. керівник В. М. Пахомова; *Укр. держ. ун-т науки і технологій*. Дніпро, 2023.

2. Пахомова В. М., Коннов М. С. Дослідження двох підходів до виявлення мережних атак із використанням нейромережної технології. *Наука та прогрес транспорту.* 2020. № 3(87). С. 81-93. URL: https://doi.org/10.15802/stp2020/208233.

3. Пахомова В. М., Павленко І. І. Дослідження параметрів якості визначення мережевих атак категорії PROBE з використанням самоорганізуючої карти. *SworldJournal*. 2022. Issue 11. Part 1. pp. 100-104. DOI: 10.30888/2663-5712.2022-11-01-022.

4. Пахомова В. М., Маслак А. В. Визначення атак категорії Probe з використанням бази даних KDDCup99 та нейронечіткої технології. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки*, 2022. Том 33(72). № 5. 135-140.

5. Пахомова В. М., Мотиленко В. А. Дослідження можливості використання RBF для визначення Smurf атак на основі бази даних KDDCup. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. Серія : Технічні науки. 2022. Т. 33 (72), № 6. С. 115–121. DOI: 10.32782/2663-5941/2022.6/20.

6. Alguliyev R. M., Aliguliyev R. M., Imamverdiyev Y. N., Sukhostat L. V. An improved ensemble approach for DoS attacks detection. *Радіоелектроніка, інформатика, управління*. 2018. № 2. С. 73-82. DOI: 10.15588/1607-3274-2018-2-8.

7. 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.

8. Esteban J. A New GHSOM Model applied to network security. *Artificial Neural Networks-ICANN 2008*. 2008. P. 680-689.

9. Grill M., Pevny T., Rehak M. Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. *Journal of Computer and System Sciences.* 2017. 83 (1). pp. 43-57. URL: https://doi.org/10.1016/j.jcss.2016.03.007.

10. 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.

11. NSL-KDD dataset. UNB: веб-сайт. URL: https://www.unb.ca/cic/datasets/nsl.html (дата звернення: 05.05.2023).

12. 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.

**Pakhomova V.M., Kvochka M.Yu. DEFINITION OF NETWORK ATTACKS OF PROBE CATEGORY BY MEANS OF MULTILAYER NEURAL NETWORK**

*To detect network attacks in real time, intrusion detection systems (Intrusion Detection System, IDS) are used, in which the problem of a large volume of network traffic appears and for solving which it is advisable to use neural network technology, which confirms the relevance of the topic. The following network attacks of PROBE category are investigated: Ipsweep; Nmap; Portsweep; Satan using the open NSL-KDD database by means of the 41-1-X-5 neural network configuration, created in the MatLAB environment using the Toolbox application, as well as determining its optimal parameters and evaluating the quality parameters for detecting network attacks of the PROBE category on the created neural network. The study of the RMS error of the created neural network with different number of hidden neurons (20, 40, 60 and 80) according to different learning algorithms (Levenberg-Marquardt, Bayesian regularization ma Scaled Conjugate Gradient) on samples of different lengths (250, 750 and 1500 examples) is carried out. It is determined that the smallest value of the error of the created neural network was achieved with 60 hidden neurons according to the Levenberg-Marquardt learning algorithm on a sample of 1500 examples. The quality parameters of detection of network attacks of PROBE category on the created neural network are evaluated. It was determined that the values of the error of the first and second kind were 6.67 % and 5.33 %, respectively.*

***Key words:*** *attack, network class, PROBE, hidden neuron, sample length, learning algorithm, error, quality assessment.*