Nakonechnyi Volodymyr, doctor of technical sciences, senior research fellow, professor at the cybersecurity and information protection academic department, Faculty Information Technologies of the Taras Shevchenko Kyiv National University, Kyiv, Ukraine.
ORCID: 0000-0002-0247-5400.
E-mail: nvc2006@i.ua

Uspenskyi Oleksandr, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.
ORCID: 0000-0001-6953-421X.
E-mail: uspensky@ukr.net.

Толюпа Сергій Васильович, доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна.

Наконечний Володимир Сергійович, доктор технічних наук, старший науковий співробітник, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна.

Успенський Олександр Анатолійович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

DOI 10.20535/2411-1031.2019.7.1.184327
УДК 004 [056.5 + 85]

АНДРІЙ ШЕВЧЕНКО,
ГЕРМАН ЗАСТЕЛО,
ЄВГЕН ШПАЧИНСЬКИЙ

АНАЛІЗ ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Проаналізовано застосування методів машинного навчання на основі штучних нейронних мереж у прикладних задачах виявлення та класифікації кіберзагроз. Актуальність тематики статі обумовлена значними обсягами впровадження технологій машинного навчання в системі захисту інформації та забезпечення кібербезпеки. Розкривається взаємозалежність між поняттями „штучний інтелект", „машинне навчання" і „глибоке навчання". За результатами аналізу інформаційних джерел, виділено основні методи машинного навчання, які знайшли застосування в галузі кібербезпеки, а саме: мережі Байєса, штучні нейронні мережі, метод опорних векторів, нечітка логіка. Проведено аналіз методів виявлення кіберзагроз, зокрема, статистичні, сигнатурні, евристичні та методи виявлення аномальній. Надано загальну характеристику й виділено переваги та завдання, які вирішують методи машинного навчання для виявлення аномальних подій у сфері кібербезпеки. Розглядаються основні типи штучних нейронних мереж, які застосовуються в задачах виявлення кіберзагроз. Підґрунтям для розгляду загального застосування методів машинного навчання є штучні нейроні мережі на основі багатошарового персептрона зі зворотнім

розповсюдженням помилки. Виділено загальну структуру штучної нейронної мережі і представлено основні математичні вирази її функціонування, розглянуто основні види функцій активації штучних нейронів, представлено загальний математичний вираз обчислення цільової функції витрат для систем машинного навчання з керованим навчанням (навчанням зі вчителем). Як вхідні для систем машинного навчання (штучних нейронних мереж) запропоновано використовувати інформативні дані індикаторів компрометації атак. Виокремлено основні дані, які можуть використовувати підсистеми моніторингу засобів захисту інформації та забезпечення кібербезпеки для виконання задач виявлення, класифікації та прогнозування інцидентів кібербезпеки. Визначено основні етапи процесу обробки даних та виявлення інцидентів кібербезпеки з використанням штучних нейронних мереж. Охарактеризовано основні системи захисту інформації та забезпечення кібербезпеки, в які впроваджують системи машинного навчання. За результатами проведеного аналізу виявлено основні проблеми їх впровадження у системи захисту інформації та забезпечення кібербезпеки, окреслено основні напрями подальших наукових досліджень. Отримані результати можуть використовуватися для визначення предметної області під час розробки та впровадження технологій машинного навчання у системи захисту інформації та кібербезпеки.

Ключові слова: машинне навчання; штучний інтелект; штучні нейронні мережі; кібербезпека; кіберзагроза; індикатори компрометації.

Постановка проблеми. Стрімкий розвиток інформаційних технологій та збільшення обсягів інформації в кіберпросторі, зробили його сучасним полем бою. Ці процеси призвели до загострення стану кібербезпеки в світі.

Сучасні кіберзагрози зумовлені спробами несанкціонованого доступу (НСД), несанкціонованої маніпуляції та модифікації інформації, які спрямовані на порушення властивостей безпеки. Для забезпечення захисту інформації від сучасних кіберзагроз їх необхідно ефективно виявляти. У багатьох засобах захисту інформації присутні підсистеми виявлення кіберзагроз, які забезпечують виокремлення та ідентифікацію кіберзагроз.

Для виокремлення та ідентифікації кіберзагроз застосовуються статистичні, сигнатурні, евристичні методи та методи виявлення аномалій [1]. Сигнатурні та статистичні методи мають обмеження функціональності і, як правило, не дозволяють виявляти нові загрози. Евристичні методи позбавлені цього недоліку та ґрунтуються на унікальній логіці, за основу якої взято комбінацію методів і експертних рішень, що потребують коригувань з часом у залежності від змін технологій застосування атак та методів НСД.

Нині активно впроваджують методи машинного навчання (МН) у системи захисту інформації та забезпечення кібербезпеки [2] - [5]. Головною причиною застосування методів МН стало те, що вони дозволяють ефективно вирішувати завдання аналізу, класифікації та прогнозування широкого класу даних, зокрема, отриманих з інформаційного середовища.

Аналіз останніх досліджень та публікацій. Тематика роботи широко висвітлена в працях зарубіжних та вітчизняних науковців. Так, наприклад, в роботах [1] - [5], [10], [11] розглядаються новітні методи й алгоритми застосування МН для вирішення загальних завдань виявлення та класифікації кібератак. Значна кількість наукових праць присвячена застосуванню методів МН у системах виявлення та попередження вторгнень [8], [9].

Застосуванню методів МН для забезпечення кібербезпеки присвячено наукові роботи [2], [12] - [11], які розглядають широкий клас методів МН у різнотипних прикладних задачах забезпечення кібербезпеки.

Метою статті є проведення аналізу застосування методів МН на основі штучних нейронних мереж (ШНМ) для вирішення задач виявлення кіберзагроз, способів застосування ШНМ та структури підсистем виявлення інцидентів порушення кібербезпеки. Для досягнення мети в роботі необхідно:

1. Проаналізувати методи МН.

2. Навести загальні математичні вирази функціонування ШНМ, які використовуються в задачах виявлення та класифікації кібернетичних загроз.

3. Розглянути основні види ШНМ, які використовуються для виявлення аномальних подій та порушень кібербезпеки.

4. Визначити основні сфери застосування ШНМ у сучасних засобах захисту інформації та забезпечення кібербезпеки.

Обмеження. В роботі обмежуємось розглядом застосування ШНМ для вирішення завдань виявлення кіберзагроз та порушень кібербезпеки. ШНМ розглядаються на прикладі багатошарового персептрона з алгоритмом зворотного розповсюдження помилки.

Викладення основного матеріалу дослідження. Останнім часом у сфері кібербезпеки широко впроваджуються технології штучного інтелекту, різновидом яких є МН. В подальшому, з ускладненням математичного апарату МН отримав розвиток новий напрям машинного навчання – глибоке навчання (*Deep learning*) [1].

Методи МН знайшли застосування в таких сферах як: медицина, робототехніка, автоматизація процесів, розпізнавання графічних і звукових образів, аналітика та передбачення процесів.

Результати аналізу останніх публікацій дозволили виділити такі математичні апарати, які відносяться до технологій МН [1] - [12]:

- мережі Байєса (*Bayesian Network*);
- штучні нейронні мережі (*ANN – Artificial Neural Network*);
- приховані марковські моделі (*HMM – Hidden Markov Model*);
- метод опорних векторів (*SVM – Support Vector Machine*);
- фільтри Калмана (*Kalman Filter*);
- методи “випадкового лісу” (*Random Forest*);
- методи на основі класифікації асоціативних правил (*Association Rule Classification*);
- дерева рішень (*Decision Trees*);
- кластеризація методом *k*-середніх (*K-means Clustering*);
- нечітка логіка (*Fuzzy Rule-Based*);
- метод *k*-найближчих сусідів (*k-nearest neighbor*).

Значна кількість цих методів не є новітніми математичними апаратами для вирішення технічних задач, оскільки вони розвиваються протягом кількох десятиліть. Проте останнім часом вони все більше застосовуються у прикладних задачах аналізу даних, у тому числі й у сфері кібербезпеки.

Сучасні кібератаки та методи НСД являють собою ланцюг складних процесів, що досить ускладнює, а інколи й унеможливлює виявлення кіберзагроз. Використання формальних методів на основі встановлених правил, сигнатурних методів, не дозволяють ефективно запобігти сучасним кіберзагрозам [1]. Сповільнене реагування на нові кіберзагрози призводить до значних втрат, блокування систем і компрометації великих обсягів конфіденційних даних.

Для більш ефективного виявлення кіберзагроз використовуються методи виявлення аномалій на основі МН. Ці методи дозволяють виявляти нові загрози на підставі складних алгоритмів аналізу даних. Одними з методів МН є методи, які ґрунтуються на використанні ШНМ. Нейронні мережі широко застосовуються в задачах виявлення, класифікації та прогнозування [1], [2], [11], [12].

ШНМ є моделлю МН, яка змінює вхідні сигнали на вихідні за допомогою нелінійних перетворень в групі штучних нейронів прихованих шарів. Суть МН на основі ШНМ полягає у навчанні (тренуванні) нейронної мережі на підставі наданого їй зразку, або без такого, для здійснення подальшої класифікації або прогнозування.

У залежності від призначення, ШНМ можуть мати у своєму складі один або декілька прихованих шарів. ШНМ, які мають більше одного прихованого шару, отримали назву багатошарового персептрона (*MLP – Multilayer Perceptron*) [14] - [16].

Розглянемо більш детально роботу ШНМ на основі багатошарового персептрона зі зворотнім розповсюдженням помилки. Кожна ШНМ складається з K шарів, кожний з яких – з N нейронів. Кількість нейронів у кожному шарі може бути різною.

Структурно шари ШНМ поділяються на вхідний, вихідний та приховані. На рис. 1 представлено тришарову ШНМ з одним вхідним шаром ($k = 1$), прихованим ($k = 2$) та вихідним шаром ($k = 3$), де k – кількість шарів ШНМ, $k \in [0, K]$.

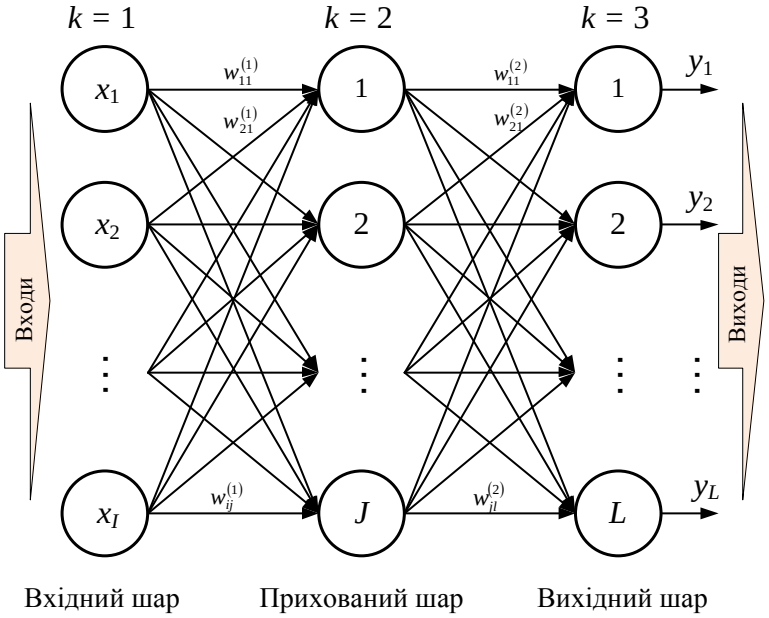


Рисунок 1 – Структура штучної нейронної мережі

Нейрони кожного шару з'єднані з усіма нейронами наступного шару. Дані ШНМ є повнозв'язними. Кожне з'єднання має власну вагу w. На вхід кожного шару подаються вхідні сигнали x, на виході нейрону отримуємо вихідні сигнали y.

Для навчання ШНМ на початковому етапі генеруються малі значення випадкових величин вагових коефіцієнтів w для кожного зв'язку між нейронами шарів. Як вхідні дані використовуються вектор вхідних даних $X_q = (x_1, x_2, \ldots, x_N)_q$ – на етапі функціонування ШНМ, та вектор навчальних зразків даних $D_q = (d_1, d_2, \ldots, d_H)_q$ – на етапі навчання ШНМ, де X_q – вектор вхідних даних, які надходять на вхід ШНМ, D_q – вектор навчальних зразків даних, які використовуються в процесі навчання ШНМ, x_N – елемент вхідних даних, d_H – елемент навчальних зразків, N – кількість входів (нейронів) у вхідному шарі, H – кількість виходів (нейронів) у вихідному шарі, q – номер зразка в навчальній вибірці X_q.

У ШНМ сигнали розповсюджуються у прямому напрямку від входу до виходу за усіма з'єднувальними лініями. Вхідні сигнали з першого шару подаються на прихований шар без перетворень. На кожен нейрон прихованого шару поступає сигнал від кожного нейрона попереднього шару [16]:

$$S_j = \sum_{i=1}^{I} x_i \cdot w_{ij} - \theta, \tag{1}$$

де S_j – зважена сума сигналів j-го нейрона;

x_i – вхідний сигнал від i-го нейрона першого (вхідного) шару;

w_{ij} – величина вагового коефіцієнта між i-м нейроном вхідного шару та i-м нейроном прихованого шару;

n – порядковий номер нейрона вхідного шару, $n \in [1, N]$;

i – порядковий номер нейрона вхідного шару, $i \in [1, I]$;

j – порядковий номер нейрона прихованого шару, $j \in [1, J]$;

θ – поріг (зміщення).

Поріг θ є параметром, еквівалентним додатковому входу x_0, і для спрощення розрахунків значенням порогу можна знехтувати.

За основу ШНМ взято принципи роботи біологічних нейронів. Штучний нейрон може знаходитись у двох станах: збудженому та незбудженому. Для переходу нейрона у збуджений стан на його вхід повинен надійти сигнал такого рівня, який би його активував. Як функцію активації в штучних нейронах використовують порогові (див. рис. 2 а) та лінійні функції, гіперболічний тангенс (див. рис. 2 в):

$$F(S) = (\beta S), \tag{2}$$

логістична функція (див. рис. 2 б), сигмоїдна функція [16]:

$$F(S) = \frac{1}{1 - e^{-S}}, \tag{3}$$

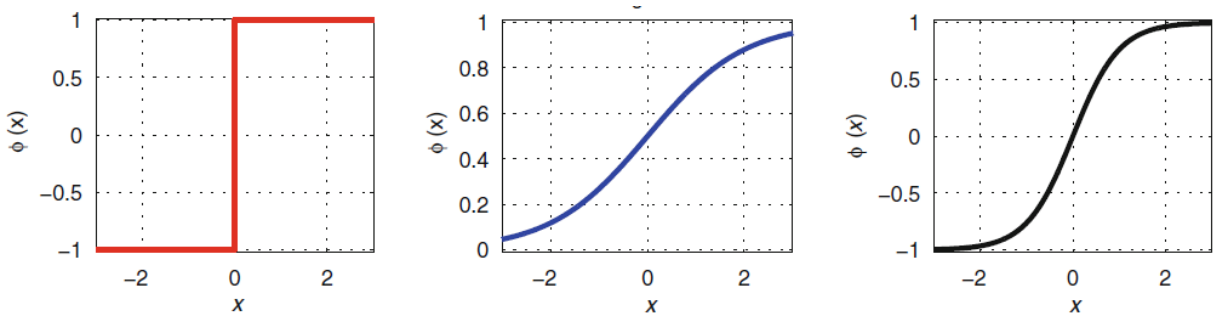
радіально-базисна активаційна функція:

$$F(S) = e^{-\frac{\|X - C\|^2}{2\sigma^2}}, \tag{4}$$

де X – вхідний вектор активаційної функції;

C – центр активаційної функції;

σ – параметр кривої Гауса.



а) б) в)

Рисунок 2 – Графіки функцій активації:
а) – порогова функція, б) – логістична функція, в) – функція гіперболічного тангенсу.

З виходів нейронів прихованого шару отримуємо результати застосування сигмоїдної функції (2) до зваженої суми сигналів j-го нейрона S_j (1). Результуюча функція вихідних сигналів набуває такого виду [16]:

$$y_j^{(k)} = F\left(\sum_{j=0}^{J} w_{ij}^{(k)} x_i^{(k-1)}\right), \tag{5}$$

де $y_j^{(k)}$ – вихідний сигнал з j-го нейрона k-го шару ШНМ;

$x_i^{(k-1)}$ – вхідний сигнал від i-го нейрона шару k-1;

$w_{ij}^{(k)}$ – величина вагового коефіцієнта між i-м нейроном k-1 шару та j-м нейроном k-го шару;

i – порядковий номер нейрона вхідного шару, $i \in [1, I]$;

j – порядковий номер нейрона прихованого шару, $j \in [1, J]$.

Суть процесу навчання для систем МН зі вчителем полягає в мінімізації цільової функції витрат (*cost function*) [1]:

$$\min_{w} J(w) = \frac{1}{2m} \sum_{p=1}^{m} \left\| y_p - \hat{y}_p \right\|^2, \quad (6)$$

де $J(w)$– цільова функція витрат;

y_p – значення вихідного сигналу, що отримано моделлю після обчислення *p*-ої вибірки тестових (тренувальних) даних;

$\hat{y}_p$ – необхідне значення сигналу на виході моделі для *p*-ої вибірки тестових даних;

w – параметри (вагові коефіцієнти) системи МН;

p – порядковий номер набору тестових даних $X_p = (x_1, x_2, \ldots, x_m)$, які використовуються для навчання моделі МН, $p \in [1, m]$;

m – загальна кількість наборів тестових даних.

У ході навчання ШНМ здійснюється корегування вагових коефіцієнтів w_{ij}, допоки досягається мінімум цільової функції витрат (6).

За результатами нелінійної обробки вектору вхідних сигналів X_q на виході ШНМ отримуємо вектор вихідних сигналів $Y_q = (y_1, y_2, \ldots, y_H)_q$. Отриманий вектор вихідних сигналів Y_q для навченої ШНМ повинен дорівнювати значенням вектора навчальних зразків D_q. В іншому випадку ШНМ повинна навчена з визначеною точністю до зазначеного результату. Суть навчання ШНМ полягає в корегуванні вагових коефіцієнтів нейронної мережі, допоки значення зразків навчання та вихідних сигналів будуть однаковими ($Y_q = D_q$).

Основними властивостями ШНМ, які використовуються в системах захисту інформації та кібербезпеки, є можливість ідентифікувати різноманітні атаки, виявляти аномальні події та зловживання в системах та мережах, здійснювати прогнозування поведінки та процесів систем.

В засобах забезпечення кібербезпеки як дані, що використовуються для виявлення та ідентифікація кіберзагроз, використовуються так звані індикатори компрометації (ІК) та індикатори атак (ІА). Безпосередньо ІК та ІА є ознаками, за якими визначають аномальну поведінку під час реагування або розслідування інциденту кібернетичної безпеки.

Визначимо, які саме данні ІК та ІА можуть бути використані ШНМ для здійснення машинного навчання. Аналіз джерел [18] - [22] дозволив виділити такі ознаки, які можуть застосовуватись у системах МН для виявлення, ідентифікації та класифікації кібератак:

- IP-адреси зловмисних джерел та С2-серверів;
- обсяги даних під час передачі та під час запитів/відповідей;
- імена і хеш-суми шкідливих файлів;
- доменні імена;
- поштові домени;
- тип контенту;
- номери портів;
- гілки реєстру;
- URL-адреси;
- протоколи;
- процеси.

Ці дані можуть використовуватися для опису аномальної поведінки та події в системі, а відповідно, в тій, чи іншій формі можуть бути надані для аналізу системами МН у засобах захисту інформації та забезпечення кібербезпеки.

Розглянемо загальний спосіб застосування ШНМ у задачах виявлення кіберзагроз. Використання ШНМ у системах виявлення та ідентифікації інцидентів кібербезпеки передбачає реалізацію таких етапів [1], [8]: збір даних, попередня обробка даних, побудова, тренування і тестування мережі, класифікація загроз (див. рис. 3).

Рисунок 3 – Процес обробки даних і виявлення інцидентів кібербезпеки з використанням ШНМ

Вхідні дані не можуть використовуватись ШНМ безпосередньо для виконання класифікації. Первинні вхідні дані потребують обробки. Під час первинної обробки вхідні данні зазнають нормалізації та стискання в залежності від потреби.

Наступним етапом є класифікація загроз, яка здійснюється шляхом виявлення та ідентифікація аномальних подій. Процедура класифікації здійснюється безпосередньо за допомогою ШНМ.

Основним етапом побудови ШНМ є етап навчання цієї штучної мережі. Класичні методи МН на основі ШНМ поділяються на методи навчання з вчителем, навчання без вчителя та навчання з підкріпленням [1]. Для вирішення завдань ідентифікації кіберзагроз, як правило, використовуються перші два методи навчання [2].

На сьогоднішній день у задачах забезпечення кібербезпеки використовують різнотипні ШНМ. Для виявлення кібератак і зловживань у комп'ютерних мережах більш широко використовують такі ШНМ [1], [2], [4] - [8], [12]:

- зі зворотнім розповсюдженням (*BP – Back-propagation*);
- з радіально-базисною функцією (*RBF – Radial Basis Function*);
- з карти, що самоорганізуються (*SOM – Self-Organizing Map*).

ШНМ зі зворотнім розповсюдженням помилки є класичним варіантом застосування нейронних мереж. Ці мережі дозволяють корегувати ваги з'єднань між нейронами шляхом визначення величини помилки між бажаним значенням виходу та реальним. Найширше ці ШНМ застосовуються в системах виявлення вторгнень [4], [8], [12].

На відміну від класичних ШНМ зі зворотнім розповсюдженням помилки, ШНМ з *RBF* мають кращу апроксимаційну здатність, добрі класифікаційні властивості та більшу швидкість навчання. ШНМ з *RBF*, як і попередній клас ШНМ, використовуються в системах виявлення вторгнень для вирішення задач ідентифікації кіберзагроз [2], [8], [12].

Методи з використанням ШНМ з картами, що самоорганізуються, є реалізацією методу навчання без вчителя. *SOM* перетворюють вхід довільної розмірності в низькорозмірні дискретні карти за допомогою методу навчання без вчителя Конохена [2], [14]. Вихідний шар ШНМ складається з нейронів, які організовані, зазвичай, у двовимірний простір. ШНМ з SOM використовуються в системах виявлення вторгнень та анти-*DDOS* системах, варіанти їх реалізації представлені в роботах [2], [7]**Помилка! Джерело посилання не знайдено.**.

Для покращення властивостей підсистем виявлення збільшені релевантності вхідних даних або їх стискання можуть бути використані в ансамблі ШНМ або різних методів МН [1], [5], [12].

Суттєвою перевагою використання ШНМ, та МН в цілому, в системах забезпечення кібербезпеки є можливість виявлення атак нульового дня. Але ШНМ, не дивлячись на чітко сформульований математичний апарат, що лежить в основі їх роботи, представляється набором взаємозв'язків з різними ваговими коефіцієнтами. Для визначення та передбачення кінцевих значень вагових коефіцієнтів та взаємозв'язків в ШНМ на сьогоднішній день не існує однозначного математичного апарату. З огляду на це, ШНМ представляє собою не що інше як „чорний ящик". Ефективність функціонування ШНМ залежить від її структури, вибору вектору вхідних даних, підбору навчальної та тестової вибірок. Тому виявлення атак нульового дня за допомогою ШНМ можливе з урахуванням значних обмежень.

На сьогоднішній час розробників засобів захисту інформації та забезпечення кібербезпеки заявляють, що вони використовують методи МН у своїх продуктах. Методи та математичний апарат, на якому грунтуються ці розробки, здебільшого не розкриваються. До основних засобів, які використовують методи МН на основі ШНМ відносяться: системи антивірусного захисту, системи виявлення та запобігання вторгненням (*IDS/IPS*), системи попередження втрати даних (*DLP*), системи управління інформаційною безпекою та подіями (*SIEM*), анти-*DDOS* системи, системи розслідування порушень кібербезпеки [1] - [12]. Їх основною особливістю є те, що в цих системах МН застосовуються в задачах інтелектуального пошуку загроз кібербезпеки.

Висновки. Сучасні методи виявлення на основі сигнатур та асоціативних правил не дозволяють виявляти нові загрози, даних про які немає в базі знань загроз. Основним недоліком методів евристичного аналізу є значна кількість хибних спрацювань та пропуску загроз. Використання методів МН у засобах захисту інформації та кібербезпеки дозволить вирішити завдання інтелектуального виявлення кіберзагроз нульового дня з більшою імовірністю. В ході роботи проаналізовано основі методи МН, які на сьогоднішній день застосовуються в системах захисту інформації та забезпечення кібербезпеки. Найбільш розповсюдженими методами МН є методи на основі ШНМ. Представлено загальний механізм обробки вхідних даних, виявлення та ідентифікації інцидентів кібербезпеки; викладено математичний апарат функціонування ШНМ на основі багатошарового персептрону в контексті загального механізму функціонування усіх методів МН.

На сьогоднішній день основними проблемами застосування методів на основі ШНМ є вибір структури ШНМ, функцій активації, методів навчання ШНМ та зразків навчальних даних. Пріоритетним напрямом є розвиток методів навчання без вчителя, що дозволить усунути недолік, який пов'язаний з залежністю від зразків навчальних даних.

У перспективах подальших досліджень планується побудова системи виявлення вторгнень на основі ШНМ, проведення навчання та тестування нейронної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] О. И. Шелухин, Д. Ж. Сакалема, и А. С. Филипова, *Обнаружение вторжений в компьютерные сети (сетевые аномалии)*. Москва, Российская Федерация: Горячая линия-Телеком, 2016.

[2] Leslie F. Sikos. *AI in Cybersecurity*. New York, USA: Springer, 2019. doi: 10.1007/978-3-319-98842-9.

[3] R. V. Yampolskiy, and M. S. Spellchecker. "Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures". [Online]. Available: https://arxiv.org/abs/1610.07997. Accessed on: Febr 08, 2019.

[4] S. Bhutada, and P. Bhutada, "Applications of Artificial Intelligence in Cyber Security", *International Journal of Engineering Research in Computer Science and Engineering*, vol. 5, iss. 4, pp. 214-219, 2018.

[5] A. Panimalar, G. Pai, and S. Khan, "Artificial Intelligence Techniques for Cyber Security", *International Research Journal of Engineering and Technology*, vol. 05, iss. 03, pp. 122-124, 2018.

[6] "Churning Out Machine Learning Models: Handling Changes in Model Predictions". [Online]. Available: https://www.fireeye.com/blog/threat-research/2019/04/churning-out-machine-learning-models-handling-changes-in-model-predictions.html. Accessed on: Febr. 08, 2019.

[7] Rasool Abdulkader A. Alfantookh, "DoS Attacks Intelligent Detection using Neural Networks", *Journal of King Saud University - Computer and Information Sciences*, vol. 18, pp. 31-51, 2006.
doi: 10.1016/S1319-1578(06)80002-9.

[8] P. Ganesh Kumar, and D. Devaraj, "Intrusion detection using artificial neural network with reduced input features", *ICTACT Journal on Soft Computing*, vol. 01, iss. 01, pp. 30-36, 2010.
doi: 10.21917/ijsc.2010.0005.

[9] M. Amini, J. Rezaeenoor, and E. Hadavandi, "Effective Intrusion Detection with a Neural Network Ensemble Using Fuzzy Clustering and Stacking Combination Method", *Journal of Computing and Security*, vol. 1, no. 4, pp. 293-305, 2014.

[10] Д. В. Ланде, І. Ю. Субач, та Ю. Є. Бояринова, *Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки*. Київ, Україна: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018.

[11] M. Stamp, *Introduction to Machine Learning with Applications in Information Security*. Boca Raton, USA : Chapman and Hall/CRC, 2018.

[12] S. Dua, and X. Du, *Data Mining and Machine Learning in Cybersecurity*. Boca Raton, USA : Chapman and Hall/CRC, 2011.

[13] Я. Гудфеллоу, И. Бенджио, и А. Курвилль, *Глубокое обучение*. Москва, Российская Федерация: ДМК Пресс, 2018.

[14] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, USA: Springer Science +Business Media, 2006.

[15] Т. Рашид, *Создаем нейронную сеть*. Санкт-Питербург, Российская Федерация: ООО «Альфа-книга», 2017.

[16] Л. Н. Ясницкий, *Интелектуальные системы*. Москва, Российская Федерация: Лаборатория знания, 2016.

[17] А. В. Федорченко, Д. С. Левшун, А. А. Чечулин, и И. В. Котенко, "Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2". *Тр. СПИИРАН*, вып. 49, с. 208-225, 2016.

[18] K. Marley, "Indicators of Compromise (IOCs): Definition and Examples". [Online]. Available: https://gadellnet.com/indicators-of-compromise. Accessed on: Febr. 08, 2019.

[19] "A definition of indicators of compromise". [Online]. Available: https://digitalguardian.com/-blog/what-are-indicators-compromise. Accessed on: Febr. 08, 2019.

[20] "IOC Security: Indicators of Attack vs. Indicators of Compromise". [Online]. Available: https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise. Accessed on: Febr. 08, 2019.

[21] "Реагирование на инциденты, признаки компрометации, оценка возможностей атакующих (Опыт ESC)". [Электронный ресурс]. Доступно: https://www.ptsecurity.com/ upload/corporate/ru-ru/ webinars/ics/Webinar_220916.pdf. Дата обращения: Июнь 08, 2019.

[22] "Как работать с данными кибербразведки: учимся собирать и выявлять индикаторы компрометации систем". [Электронный ресурс]. Доступно: https://habr.com/ru/company/ solarsecurity/blog/438798. Дата обращения: Февр. 08, 2019.

[23] "CS229 – Machine Learning". [Online]. Available: https://see.stanford.edu/Course/CS229. Accessed on: Febr. 08, 2019.

[24] K. Al-Nafjan, M. A. Al-Hussein, A. S. Alghamdi, M. A. Haque, and I. Ahmad, "Intrusion detection using PCA based modular neural network", *International Journal of Machine Learning and Computing*, vol. 2, no. 5, pp. 583-587, 2012.
doi: 10.7763/IJMLC.2012.V2.194.

Стаття надійшла до редакції 10.03.2019.

REFERENCE

[1] O. Shelukhin, D. Sakalema, and A. Filipova, *Intrusion detection in computer networks (network anomalies)*. Moskow, Russia: Hotline-Telecom, 2016.

[2] Leslie F. Sikos. *AI in Cybersecurity*. New York, USA: Springer, 2018. doi: 10.1007/978-3-319-98842-9.

[3] R. V. Yampolskiy, and M. S. Spellchecker. "Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures". [Online]. Available: https://arxiv.org/abs/1610.07997. Accessed on: Febr 08, 2019.

[4] S. Bhutada, and P. Bhutada, "Applications of Artificial Intelligence in Cyber Security", *International Journal of Engineering Research in Computer Science and Engineering*, vol. 5, iss. 4, pp. 214-219, 2018.

[5] A. Panimalar, G. Pai, and S. Khan, "Artificial Intelligence Techniques for Cyber Security", *International Research Journal of Engineering and Technology*, vol. 05, iss. 03, pp. 122-124, 2018.

[6] "Churning Out Machine Learning Models: Handling Changes in Model Predictions". [Online]. Available: https://www.fireeye.com/blog/threat-research/2019/04/churning-out-machine-learning-models-handling-changes-in-model-predictions.html. Accessed on: Febr. 08, 2019.

[7] Rasool Abdulkader A. Alfantookh, "DoS Attacks Intelligent Detection using Neural Networks", *Journal of King Saud University - Computer and Information Sciences*, vol. 18, pp. 31-51, 2006. doi: 10.1016/S1319-1578(06)80002-9.

[8] P. Ganesh Kumar, and D. Devaraj, "Intrusion detection using artificial neural network with reduced input features", *ICTACT Journal on Soft Computing*, vol. 01, iss. 01, pp. 30-36, 2010. doi: 10.21917/ijsc.2010.0005.

[9] M. Amini, J. Rezaeenoor, and E. Hadavandi, "Effective Intrusion Detection with a Neural Network Ensemble Using Fuzzy Clustering and Stacking Combination Method", *Journal of Computing and Security*, vol. 1, no. 4, pp. 293-305, 2014.

[10] D. Land, I. Subach, and Y. Boyarinova, *Fundamentals of the theory and practice of intellectual data analysis in the field of cybersecurity*. Kyiv, Ukraine: ISZZI Igor Sikorsky Kyiv Polytechnic Institute, 2018.

[11] M. Stamp, *Introduction to Machine Learning with Applications in Information Security*. Boca Raton, USA : Chapman and Hall/CRC, 2018.

[12] S. Dua, and X. Du, *Data Mining and Machine Learning in Cybersecurity*. Boca Raton, USA : Chapman and Hall/CRC, 2011.

[13] J. Goodfellow, I. Bengio, and A. Courville, *Deep learning*. Moskow, Russia: DMK Press, 2018.

[14] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, USA: Springer Science +Business Media, 2006.

[15] T. Rashid, *Create a neural network*. Saint Petersburg, Russia: Alfa-Kniga LLC, 2017.

[16] L. Yasnitsky, *Intellectual systems*. Moskow, Russia: Laboratory of knowledge, 2016.

[17] A. Fedorchenko, D. Levshun, A. Chechulin, and I. Kotenko, "Analysis of methods for correlating security events in SIEM systems. Part 2", *Tr. SPIIRAN*, iss. 49, pp. 208-225, 2016.

[18] K. Marley, "Indicators of Compromise (IOCs): Definition and Examples". [Online]. Available: https://gadellnet.com/indicators-of-compromise. Accessed on: Febr. 08, 2019.

[19] "A definition of indicators of compromise". [Online]. Available: https://digitalguardian.com/-blog/what-are-indicators-compromise. Accessed on: Febr. 08, 2019.

[20] "IOC Security: Indicators of Attack vs. Indicators of Compromise". [Online]. Available: https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise. Accessed on: Febr. 08, 2019.

[21] "Incident response, signs of compromise, assessment of the capabilities of the attackers (ESC Experience". [Online]. Available: https://www.ptsecurity.com/upload/corporate/ru-ru/ webinars/ics/ Webinar_220916.pdf. Accessed on: Febr. 08, 2019.

[22] "How to work with cyber prospecting data: learn to collect and detect indicators of system compromise". [Online]. Available: https://habr.com/ru/company/solarsecurity/blog/438798. Accessed on: Febr. 08, 2019.
[23] "CS229 – Machine Learning". [Online]. Available: https://see.stanford.edu/Course/CS229. Accessed on: Febr. 08, 2019.
[24] K. Al-Nafjan, M. A. Al-Hussein, A. S. Alghamdi, M. A. Haque, and I. Ahmad, "Intrusion detection using PCA based modular neural network", *International Journal of Machine Learning and Computing*, vol. 2, no. 5, pp. 583-587, 2012. doi: 10.7763/IJMLC.2012.V2.194.

ANDRII SHEVCHENKO,
HERMAN ZASTELO,
YEVHENII SHPACHINSKIY

ANALYSIS OF APPLICATION A METHODS OF MACHINE LEARNING BASED ON ARTIFICIAL NEURAL NETWORKS IN THE TASKS OF DETECTING CYBERSECURITY THREATS

The article analyzes the application of methods of machine learning based on artificial neural networks in applied problems of detection and classification of cyber threats. The topic of gender is associated with a significant increase in the implementation of the information technology and cybersecurity technologies of the machine learning. The interdependence between the concepts of "artificial intelligence", "machine learning", "deep learning" is revealed. In the article, according to the results of the information sources analysis, the main methods of ML, which have been used in the field of cybersecurity, as follows: Bayes' networks, artificial neural networks, support vector machine, fuzzy logic, and others are highlighted. A brief analysis of methods for detecting cybersecurity threats using information security and cybersecurity, as follows: statistical, signature, heuristic and abnormal detection methods, has been carried out. The general characteristic is given and the advantages and problems that solve the ML methods for the detection of abnormal events are outlined. The paper considers the main types of artificial neural networks that are used in the tasks of detecting cyber threats. In the article, the basis for considering the general application of machine learning methods is taken by artificial neural networks based on multilayered perceptron with a backpropagation. The general structure of artificial neural networks is selected and the basic mathematical expressions of its functioning are presented, the basic types of activation functions of artificial neurons are considered, the general mathematical expression of the calculation cost function for unsupervised machine learning is presented. More substantially consider the issues of the input data choice for systems machine learning (artificial neural networks). It is proposed to use informative data of attack compromise indicators as input to machine learning systems (artificial neural networks). The main data that can be used by the monitoring subsystem of information security and cyber defense can be used to perform detection, classification and forecasting incidents of cybernetic security. The main stages of the process of data processing and detection of cybersecurity incidents using the (artificial neural networks) are identified. The main systems of information protection and cybersecurity in which machine learning systems are implemented are described. According to the results of the article, the main implementation problems of the machine learning methods in the information security systems are highlighted, the main directions of further scientific research are outlined. This work can be used to highlight the subject area during the development and implementation of machine learning technologies in information security and cybersecurity systems.

Keywords: machine learning; artificial intelligence; artificial neural networks; methods of anomalies detection; detection of cyber threats; cybersecurity.

Шевченко Андрій Сергійович, кандидат технічних наук, старший аналітик групи моніторингу та реагування на кіберінциденти, ТОВ Метінвест Діджитал, Київ, Україна.

ORCID: 0000-0001-7991-0119.

E-mail: acweva@gmail.com.

Застело Герман Ігорович, кандидат технічних наук, доцент, доцент кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0001-7306-4898.

E-mail: girzov66@gmail.com.

Шпачинський Євген Олександрович, слухач, Інститут інформаційних технологій, Національний університет оборони України імені Івана Черняховського, Київ, Україна.

ORCID: 0000-0002-6189-4218.

E-mail: shpachinskiy1942@gmail.com.

Shevchenko Andrii, candidate of technical sciences, security operation center senior analyst, Metinvest Digital Ltd., Kyiv, Ukraine.

Zastelo Herman, candidate of technical sciences, associate professor, associated professor of Information and cyber defense academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Shpachinskiy Yevhen, student, Institute of information technologies, The National defence university of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine.