МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації
(назва факультету, інституту)

Систем інформаційного та кібернетичного захисту
(назва кафедри)

"На правах рукопису"

«До захисту допущено»
Завідувач кафедри
Савченко В. А.
(підпис) (ініціали, прізвище)
"____" _____ 202_р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 Кібербезпека
(код та назва спеціальності)

на тему: Використання штучних нейромереж в цілях забезпечення безпеки інформації

Студент групи СЗДМ – 61 Рєзнік Денис Володимирович _____
(шифр групи) (прізвище, ім'я, по батькові) (підпис)

Керівник к.т.н., Ахрамович Володимир Миколайович _____
(вчені ступінь та звання, прізвище, ініціали) (підпис)

Нормоконтроль: _____ _____
(вчені ступінь та звання, прізвище, ініціали) (підпис)

Київ – 2021

ЗАТВЕРДЖУЮ»

Завідувач кафедри

_____ Савченко В. А.
(підпис) (ініціали, прізвище)

“__” _____ 2021р.

ЗАВДАННЯ

на атестаційну роботу магістра

студенту Рєзніку Денису Володимировичу
(прізвище, ім’я, по батькові)

1. Тема роботи: Використання штучних нейромереж в цілях забезпечення безпеки інформації

Затверджена наказом по університету від “__” _____ 202_ р. №_____

2. Термін здачі студентом оформленої роботи “____”_____202_ р.

3. Об’єкт дослідження: Штучні нейромережі

4. Предмет дослідження: Використання штучних нейромереж в цілях забезпечення безпеки інформації

5. Мета роботи: Обґрунтування необхідності впровадження штучних нейромереж для забезпечення захисту інформації

6. Перелік питань, які мають бути розроблені:

7. Перелік публікацій:

8. Перелік ілюстративного матеріалу:

9. Дата видачі завдання “__” _____ 202_ р.

Керівник _____ Ахрамович В. М.
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Рєзнік Д.В.
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	**Примітка**
1	Підбір науково-технічної літератури		
2	Обґрунтування актуальності теми роботи		
3	Написання першого розділу роботи		
4	Написання другого розділу роботи		
5	Написання третього розділу роботи		
6	Написання висновків по роботі		
8	Підготовка демонстраційних матеріалів		
9	Підготовка доповіді		
10	Захист в ДЕК		

Студент _____ Рєзнік Д.В.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Ахрамович В. М.
(підпис) (ініціали, прізвище)

ЗМІСТ

ВСТУП ……..…….……..…..

АНОТАЦІЯ……..
ANNOTATION …….…….....
РОЗДІЛ 1 ШТУЧНІ НЕЙРОМЕРЕЖІ
1.1 Принципи роботи нейромережі ……..…..…….....

1.2 Класифікація штучних нейромереж……..…….....

РОЗДІЛ 2 ЗАГРОЗИ КІБЕРБЕЗПЕКИ...……..……
2.1 Історія розвитку 4G …….……....…….
2.2 Принципи побудови і функціонування мереж 4G …….……..
2.3 Сучасний стан нейромереж…….……....…...
РОЗДІЛ 3 ПЕРЕВАГИ ПРИ ВИКОРИСТАННІ ШТУЧНИХ НЕЙРОМЕРЕЖ В КІБЕРБЕЗПЕЦІ ……....
3.1 Основні принципи навчання нейромереж ……..……....
3.2 Етапи вирішення задач за допомогою нейромереж ...……..…...
3.3 Переваги нейромереж …….
РОЗДІЛ 4 ОХОРОНА ПРАЦІ …….…….…....
ВИСНОВКИ …….
СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ …….

ВСТУП

В наш час комп'ютерні мережі являють собою великі розподілені системи програм та пристроїв, що взаємодіють між собою, щоб обмінюватися інформацією, а також зберігати її та обробляти. Мережі поєднують різні типи пристроїв, з'єднаних каналами зв'язку. Посилення навантаження мереж, їх ускладнення, зростання виникнення методів порушення роботи, створюють необхідність серйозного ставлення до проблем мережевої безпеки.

Більшість існуючих систем виявлення атак (СВА), що застосовуються для моніторингу безпеки інформаційних систем (ІС), засновані на використання правил і сигнатур, за допомогою яких аналізується вектор вхідних даних і на підставі чого робиться висновок про наявність або відсутність атаки. При найменшому відхиленні сигнатури атаки від сигнатури або правила, що є в базах даних (БД), ця атака не буде виявлена. Тому через велику різноманітність атак звичайні СВА не завжди здатні забезпечити ідентифікацію атаки. Одним із варіантів вирішення цієї проблеми може бути використання штучних нейромереж в цілях забезпечення інформаційної безпеки.

З розвитком інформаційних систем та його якісного ускладнення їм делегується дедалі більше функцій, властивих виключно людині. У багатьох процесах людина перестала конкурувати з машиною, навіть функції управління інформацією вже не є ексклюзивними для неї. Саме через вдосконалення технічної бази, та можливість втілення в реальність більш ранніх теорій що-до створення штучних нейромереж (ШНМ) на сьогоднішній день дана тема набуває високої актуальності. Метою даної роботи є обґрунтування необхідності впровадження ШНМ для забезпечення захисту інформації.

АНОТАЦІЯ

Метою магістерської кваліфікаційної роботи є обґрунтування необхідності впровадження штучних нейромереж для забезпечення захисту інформації. Ця проблема є досить актуальною, оскільки в наш час проблема кібератак є не тільки одною з найважливіших, але й приносить величезні фінансові збитки. Саме тому в даній роботі доводиться необхідність впровадження штучних нейромереж в цілях захисту інформації.

SUMMARY

The purpose of the master's qualification work is to substantiate the need for the introduction of artificial neural networks to ensure the protection of information. This problem is quite relevant, because in our time the problem of cyber-attacks is not only one of the most important, but also brings huge financial losses. That is why this paper proves the need for the introduction of artificial neural networks in order to protect information.

РОЗДІЛ 1.
ШТУЧНІ НЕЙРОМЕРЕЖІ

1.1 Принципи роботи нейромережі.

На даний момент під ШНМ розуміють математичну модель, а також її програмне

чи апаратне втілення, побудоване за принципом організації та функціонування біологічних нейронних мереж – мереж нервових клітин живого організму [26]. Автором пропонується уточнення цього поняття як «система що складається з математичної моделі, і навіть її програмно-апаратної втілення». Саме об'єднання програмної та апаратної складової можна назвати повноцінною ШНМ, а не імітацією її діяльності більш примітивної елементарної базі, чи структурної, але з функціональної машиною працює на подібній архітектурі. Це є необхідним, оскільки найбільш просунуті ШНМ на сьогодні є саме програмно-апаратними комплексами та його розвиток бачиться найперспективнішим.

Хоча протягом тривалого часу технічна база не дозволяла втілити та перевірити практично теоретичні дослідження. Також необхідно зазначити, що до другої половини 80-х розробки, які велися в цій галузі були здебільшого тільки теоретичними, і лише починаючи з недавнього часу їх почали перетворювати у реальні діючі зразки. Починаючи з 1986-го року почали з'являтися стабільно працюючі ШНМ, які дозволили на практиці вивчити і, згодом модернізувати нейромережі.

Кожен нейрон характеризується своїм поточним станом за аналогією з нервовими клітинами головного мозку, які можуть бути збуджені або загальмовані. Він має групу синапсів - односпрямованих вхідних зв'язків, з'єднаних з виходами інших нейронів, а також має аксон - вихідний зв'язок даного нейрона, з якого сигнал (збудження або гальмування) надходить на синапс наступних нейронів. Загальний вигляд нейрона наведено на рис. 1.

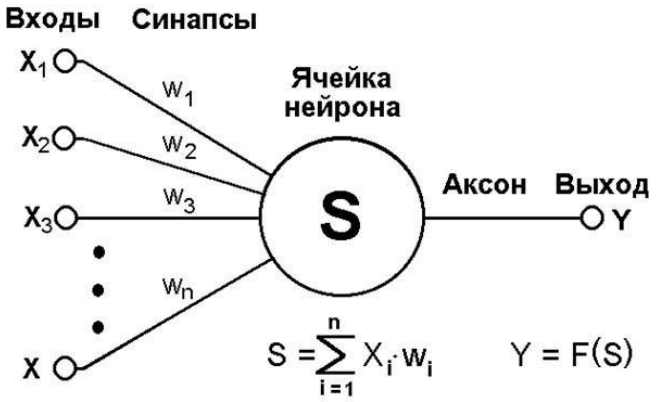

рис.1

Для НМ вводиться функція, що визначає поріг спрацьовування Y = F(S)

В даний час найчастіше використовують багатошарові архітектури нейронних мереж. Зазвичай така мережа складається з вхідного шару, одного або кількох прихованих шарів та вихідного шару. Багатошарова мережа зображена на рис. 2.

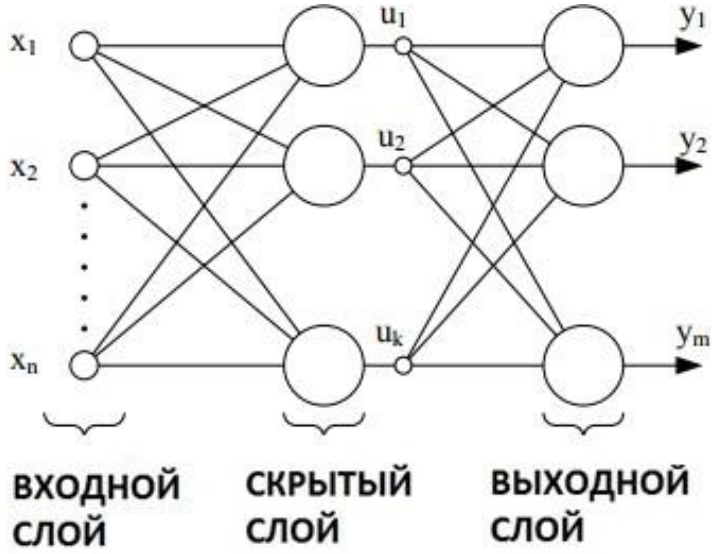

рис.2

Можна виділити такі найпоширеніші архітектури НМ:

• мережі прямого розповсюдження, в яких усі зв'язки НМ спрямовані строго від вхідного шару до вихідного;

• мережі зворотного розповсюдження, коли сигнал може передаватися назад до вхідного шару;

• мережа Кохонена – мережа з певним шаром (шар Кохонена), таким, що сигнали цього шару обробляються за правилом «переможець забирає все»,

причому, найбільшому сигналу присвоюється одиниця, інші сигнали звертаються в нуль [23].

Вибір структури НМ здійснюється відповідно до особливостей та складності завдання. Застосування НМ для вирішення будь-якого завдання включає два етапи: етап навчання та етап розпізнавання. На етапі навчання на вхід НМ подається навчальна вибірка, що складається із заздалегідь відібраних та підготовлених вхідних та вихідних векторів [27]. Відповідно до обраного алгоритму навчання відбувається налаштування вагових коефіцієнтів, в результаті якої при подачі на вхід НМ навчального вектора на виході з'являється заданий вихідний вектор, що позначає клас вхідного вектора.

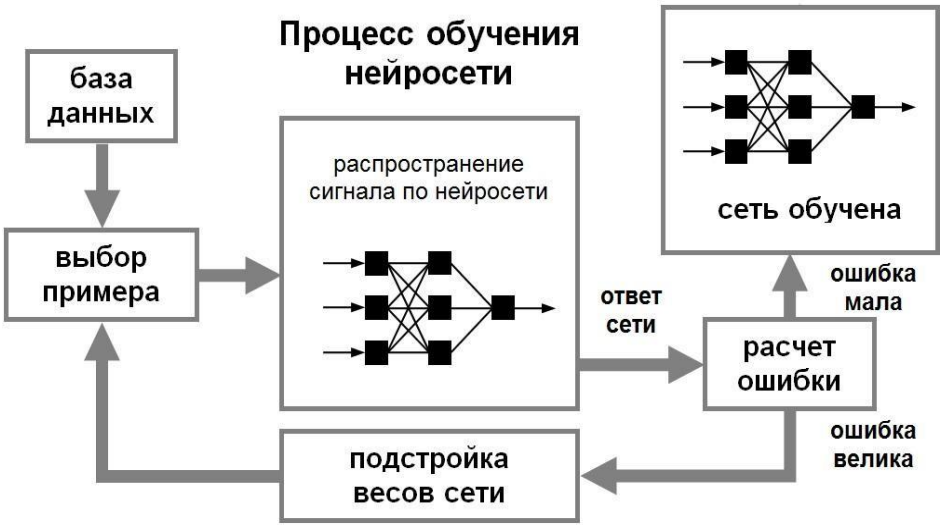

рис.3

На етапі розпізнавання на ВШ надходить заздалегідь невідомий вхідний вектор. При цьому на виході з'являється вектор – результат розпізнавання, відповідно до якого вхідний вектор зараховується до одного з найвідоміших класів.

Найбільш важлива перевага нейронних мереж при виявленні зловживань – їх здатність вивчати характеристики навмисних атак та ідентифікувати елементи, не схожі на ті, що спостерігалися в мережі.

Після того як нейронна мережа навчена безліччю послідовних команд системи, що захищається, або однією з її підсистем, мережа є «образом» нормальної поведінки. Процес виявлення аномалій є визначенням показника

неправильно передбачених команд, тобто фактично виявляється відмінність у поведінку об'єкта.

Класифікація розв'язуваних завдань у галузі даного методу ШІ:

• Швидке розпізнавання загроз;

• Боротьба зі шкідливим ПЗ, яке так само самонавчається.

• Винесення певних відомостей у процесі навчання та побудова на їх основі більш потужної системи захисту.

1.2 Класифікація штучних нейромереж

Залежно від типу міжнейронних зв'язків розрізняють ШНМ:

- із прямими зв'язками (рис.4);

- з перехресними зв'язками;

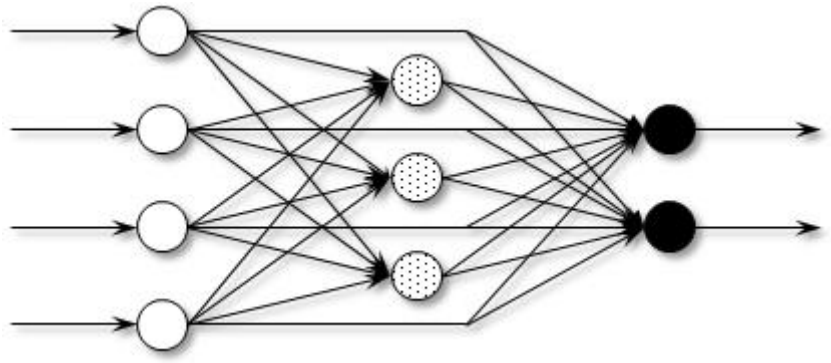

рис.4

- зі зворотними (рекурентними) зв'язками (рис.5). У таких мережах нейрон може посилати сигнали сам собі, нейронам того ж шару або нейронам попередніх шарів.

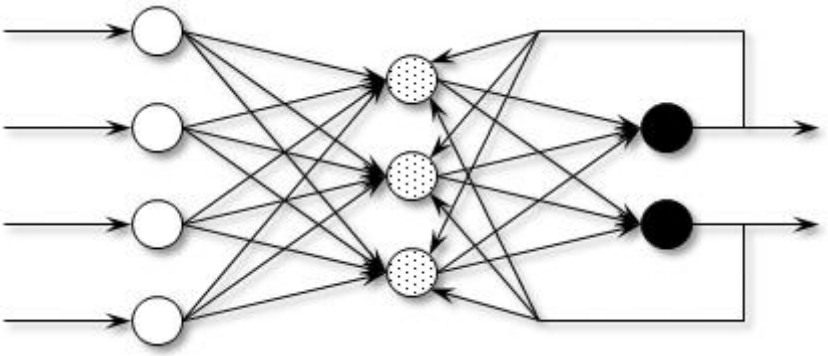

рис.5

Перед безпосереднім використанням, тобто. Перед вирішенням конкретної задачі розпізнавання образів, необхідно налаштувати (навчити) мережу. Процес навчання мережі полягає у визначенні набору зв'язків та коефіцієнтів зв'язків між нейронами. Залежно від способу навчання розрізняють такі типи ШНМ:

- які навчаються з учителем (контрольоване або спостерігається навчання). Під час навчання з учителем всі приклади навчальної вибірки містять правильні відповіді (виходи), відповідні вихідним даним (входам). У процесі навчання ваги (коефіцієнти) налаштовуються те щоб мережа породжувала відповіді, найбільш близькі до правильним;

- які навчаються без вчителя (неконтрольоване або неспостерігаєме. навчання). Навчання без вчителя використовується, коли для всіх прикладів навчальної вибірки відомі правильні відповіді. У цьому випадку робляться спроби визначення коефіцієнтів мережі з метою визначення категорій (класів) зразків та подальшого їх розподілу за категоріями. Використовується, зокрема, на вирішення завдань кластеризації;

- зі змішаним (гібридне) навчанням. При змішаному навчанні частина терезів визначається за допомогою навчання з учителем, а інша частина виходить за допомогою алгоритмів самонавчання.

Залежно від правила корекції коефіцієнтів (wi) ШНМ ділять на такі категорії:

- правило корекції помилково (дельта-правило). Різниця між відомим значенням результату та реакцією мережі використовується для коригування вагових коефіцієнтів. Коригування полягає в невеликому (зазвичай менше 1%) збільшенні ваг тих зв'язків, які посилюють правильні реакції, та зменшенні ваги тих зв'язків, які сприяють помилковим. Зазвичай використовується для одношарових мереж;

- Правило зворотного поширення помилки. При навчанні коригування поширюється назад по мережі на всі вагові коефіцієнти. Зазвичай використовується для багатошарових мереж. У разі коли коригування вагових

коефіцієнтів виконується після прогону одного образу, говорять про послідовний режим навчання. режим, коли коригування виконується не відразу, а після прогону кількох навчальних образів, називається пакетним (правило зворотного поширення помилки у часі);

- Синхронне навчання (правило Хебба). Це правило спирається на наступні нейрофізіологічне спостереження: якщо нейрони з обох боків синапс активізуються одночасно і регулярно, то сила синаптичного зв'язку зростає. Таким чином, коригування підлягають коефіцієнти тільки тих зв'язків, вихід яких відмінний від нуля;

- Конкурентне навчання (правило Кохонена, «переможець забирає все»). У кожному шарі коригуються вагові коефіцієнти лише одного нейрона-переможця, у якого вихід найточніше відповідає пред'явленому зразку;

- правило Больцмана. Алгоритм навчання заснований на ідеї моделювання відпалу - способу випалювання дефектів у кристалічній решітці. Атоми, що займають у ній неправильне місце, за низької температури що неспроможні зміститися у потрібне становище - їм не вистачає кінетичної енергії подолання потенційного бар'єру. При цьому система загалом перебуває у стані локального енергетичного мінімуму. Для виходу з нього метал нагрівають до високої температури, а потім повільно охолоджують, дозволяючи атомам зайняти правильні положення у ґратах, що відповідає глобальному мінімуму енергії. Імітація відпалу в нейронній мережі виконується за такою процедурою:

- на вхід мережі подається навчальний образ та обчислюється вихід;

- обчислюється значення середньої квадратичної помилки між бажаним та отриманим вихідними векторами;

- вагові коефіцієнти зміняться випадковим чином, потім обчислюються новий вихід та результуюча помилка. Якщо помилка зменшилася, залишають змінені ваги; якщо помилка збільшилася, залишають змінені ваги з ймовірністю, що визначається розподілом Больцмана. Якщо помилка залишилася незмінною, то вагові коефіцієнти повертають для її попереднього значення.

РОЗДІЛ 2
ЗАГРОЗИ КІБЕРБЕЗПЕКИ

2.1 Основні загрози кібербезпеки

Загальні джерела кіберзагроз, яких відносять кілька поширених джерел для організаций:

- Національні держави - ворожі країни можуть запускати кібератаки на місцеві компанії та установи з метою завадити комунікації, викликати заворушення та завдати шкоди.

- Терористичні організації – терористи проводять кібератаки, спрямовані на руйнування чи зловживання критично важливою інфраструктурою, загрожують національній безпеці, підривають економіку та завдають тілесних ушкоджень громадянам.

- Злочинні групи. Організовані групи хакерів прагнуть зламати комп'ютерні системи з одержання економічної вигоди. Ці групи використовують фішинг, спам, шпигунське та шкідливе ПЗ для вимагання, крадіжки приватної інформації та онлайн-шахрайства.

- Хакери - окремі хакери орієнтовані організації, використовуючи різні методи атак. Зазвичай вони мотивовані особистою вигодою, помстою, фінансовою вигодою чи політичною діяльністю. Хакери часто розробляють нові загрози, щоб підвищити свої кримінальні здібності та покращити своє особисте становище у хакерському співтоваристві.

- Шкідливі інсайдери – співробітник, який має законний доступ до активів компанії та зловживає своїми привілеями для крадіжки інформації чи пошкодження комп'ютерних систем з метою економічної чи особистої вигоди. Інсайдери можуть бути співробітниками, підрядниками, постачальниками чи партнерами цільової організації. Вони також можуть бути сторонніми, які

зламали привілейований обліковий запис та видають себе за його власника [3,7]. Типи загроз кібербезпеці Атаки шкідливого ПЗ

Шкідливе ПЗ - це ПЗ, яке включає віруси, черв'яки, трояни, шпигунське ПЗ та програми-вимагачі, і є найбільш поширеним типом кібератак. Шкідливе програмне забезпечення проникає в систему, як правило, через посилання на ненадійному веб-сайті або електронною поштою або через завантаження небажаного програмного забезпечення. Він розгортається в цільовій системі, збирає конфіденційні дані, маніпулює та блокує доступ до компонентів мережі, а також може знищити дані або повністю вимкнути систему [7-10].

Ось деякі з основних типів атак шкідливих програм:

- Віруси – фрагмент коду впроваджується у додаток. Коли програма запускається, запускається шкідливий код.

- Черв'яки - шкідливе ПЗ, яке використовує вразливість програмного забезпечення та бекдори для отримання доступу до операційної системи. Після встановлення в мережі черв'як може виконувати такі атаки, як розподілена відмова в обслуговуванні (DDoS).

- Трояни - шкідливий код або програмне забезпечення, яке видає себе за безневинну програму, що ховається в програмах, іграх або вкладеннях електронної пошти. Користувач, який нічого не підозрює, завантажує троян, дозволяючи йому отримати контроль над своїм пристроєм.

- Програма-вимагач - користувачеві або організації заборонено доступ до їх власних систем або даних за допомогою шифрування. Зловмисник зазвичай вимагає сплати викупу в обмін на ключ дешифрування для відновлення доступу, але немає гарантії, що сплата викупу фактично відновить доступ або функціональність.

- Криптоджекінг - зловмисники розгортають програмне забезпечення на пристрої жертви і без їхнього відома починають використовувати свої обчислювальні ресурси для генерації криптовалюти. Зачеплені системи можуть стати повільними, а комплекти криптоджекінгу можуть вплинути на стабільність системи.

- Шпигунське ПЗ - зловмисник отримує доступ до даних користувача, що нічого не підозрює, включаючи конфіденційну інформацію, таку як паролі та платіжні реквізити. Шпигунське програмне забезпечення може вплинути на настільні браузери, мобільні телефони та настільні програми.

- Рекламне ПЗ - активність користувача в браузері відстежується визначення моделей поведінки та інтересів, що дозволяє рекламодавцям розсилати користувачеві цільову рекламу. Рекламне ПЗ пов'язане зі шпигунським ПЗ, але не вимагає встановлення програмного забезпечення на пристрій користувача і не обов'язково використовується в зловмисних цілях, але може використовуватися без згоди користувача та ставити під загрозу його конфіденційність.

- Безфайлове шкідливе програмне забезпечення - в операційній системі не встановлено програмне забезпечення. Власні файли, такі як WMI та PowerShell, редагуються для увімкнення шкідливих функцій. Цю приховану форму атаки важко виявити (антивірус не може її ідентифікувати), оскільки компрометовані файли розпізнаються як легітимні.

- Руткіти – програмне забезпечення впроваджується в програми, прошивки, ядра операційних систем або гіпервізори, забезпечуючи віддалений адміністративний доступ до комп'ютера. Зловмисник може запустити операційну систему у скомпрометованому середовищі, отримати повний контроль над комп'ютером та доставити додаткове шкідливе ПЗ [4].

2.2 Сучасні методи боротьби з кіберзагрозами

Існуючі на сьогоднішній день системи ІБ мають одну спільну рису - це постійність висновків. При цьому недоліки зловмисники завжди можуть розраховувати на проникнення в систему за наявності досить потужної техніки і часу на підбір ключа. У такому разі виникає необхідність у системі з випадковим отриманням результату та багаторазовими перевірками на допуск до інформації, саме цим ШНМ вигідно відрізняються від статичних систем ІБ

(навіть за наявності регулярних оновлень та зміни крипт ключів). Хоча в наш час залишається потреба в особі, яка приймає рішення, надалі цю функцію можна буде перекласти на машину.

При поточних темпах розвитку обчислювальної техніки, а також теорії та практики розвитку штучного інтелекту необхідно очікувати дедалі більшої автоматизації у сфері як кіберзахисту, і кібернападу. На сьогоднішній день існує кілька основних загроз кібербезпеці. За даними доповіді IBM з аналізу кіберзагроз за 2016–2019 роки основною та найнебезпечнішою загрозою інформаційної безпеки підприємств є APTатаки [7]. Метою такої атаки є комп'ютер із найважливішою інформацією, але розпочатися все може з незначного зараження рядової машини.

Яскравим прикладом може бути успішна APT-атака на інформаційну мережу газети The New York Times [8]. Також необхідно відзначити найбільш гучні атаки на Пентагон, NASA, і міністерство енергетики США в 1998-2000 роках [9], напад на Los Alamos National Laboratory [10], GhostNet - найбільша акція кібершпигунства, в ході якої було заражено більше 1000 комп'ютерних мереж, у тому числі урядових, у більш ніж 100 країнах [11].

Виділяють чотири стадії APT-атаки: підготовка, проникнення, поширення, досягнення мети, кожна з яких супроводжується діяльністю, спрямованою на приховування слідів присутності у системі. Також необхідно зазначити, що на підготовчому етапі проникнення можлива участь психологів, соціальних інженерів та інших спеціалістів із роботи з людьми. Схема APT-атаки зображена на рис.6.

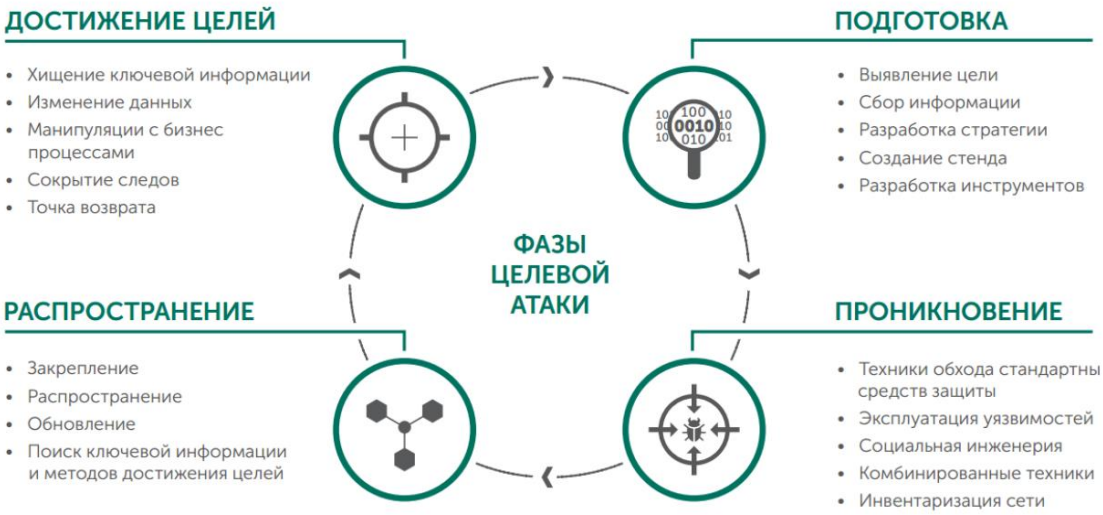

рис.6

Вже 12 травня 2017 відбулася атака з використанням штучної нейромережі з впровадженням вірусу відомого як WannaCry. Одними з перших атакували комп'ютери в Іспанії, а потім і в інших країнах. Серед них за кількістю заражень лідирували Росія, Україна та Індія. Загалом за короткий час від вірусу постраждало понад 500 тисяч комп'ютерів, що належать приватним особам, комерційним організаціям та урядовим установам практично у всіх країнах світу [13]. Поширення вірусу блокувало роботу багатьох організацій по всьому світу: лікарень, аеропортів, банків, заводів та ін.

Зокрема, у низці британських госпіталів було відкладено виконання призначених медичних процедур, обстежень та термінових операцій. Хоча спочатку вірус був призначений для вимагання фінансових коштів, згодом він був використаний для отримання інформації, що становить комерційну таємницю, як, наприклад, у випадку з підприємствами Renault. Сам хробак WannaCry був створений і запущений невідомими зловмисниками за допомогою вкраденої у Агенції Національної Безпеки США інформації [14]. Основним підозрюваним вважається хакерське угруповання Lazarus Group, ймовірно пов'язане з урядом КНДР [15].

Необхідно відзначити, що на етапі підготовки атак хакерів вже зараз багато зловмисників використовують нейромережі для моделювання дій служби безпеки компаній на тестових стендах і таким чином планування і

здійснення атак стає більш продуманим і набуває великих шансів на успіх. Зі сказаного вище очевидною є необхідність у прийнятті адекватних заходів для парірування загрози, що виходить від зловмисників, які використовують ШНМ у своїх цілях. Тому для парірування таких загроз необхідно використовувати як програмно-технічні комплекси, так і людей, діяльність яких буде зосереджена на пошуку, виявленні та протидії даних порушників.

Насамперед варто врахувати, що сконструйовані для цієї мети ШНМ повинні пройти багаторазову перевірку на випробувальних стендах з метою визначення їх вразливостей та точності виконання завдань. Також не можна забувати про те, що при одних і тих же вихідних даних результат, що видається ШНМ, може бути різним, і саме тому потрібна наявність операторів, які контролюватимуть роботу такого програмно-апаратного комплексу.

Необхідно відзначити, що існуючі на сьогоднішній день системи захисту інформації складаються з безлічі вузькоспеціалізованих програм та спеціальної апаратури, а також вимагають штату співробітників кількох спеціальностей для своєї роботи. У цьому плані шнм вигідно відрізняються від сучасних систем тим, що вони не вимагають великої кількості співробітників і є в повному розумінні програмно-апаратними комплексами, таким чином вимагають менше ресурсів на свою підтримку.

Перша лінія оборони – захист від DDoS

Захист від DDoS DoS (Denial of Service) - атака на обчислювальну систему з метою довести її до відмови. Вектори атак DDoS:

• Volumetric – об'ємні атаки (UDP, ICMP, SYN флуд, DNS Amplification);

• Low-And-Slow – повільні, але небезпечні атаки (HTTP POST/GET flood, Slowloris).

Як правило, для DDoS використовують IP spoofing (підміну адреси відправника) пакети. Іноді DDoS це лише прикриття. Боротьба з DDoS атакою – це відкидання нелегітимних пакетів та пропуск легітимного трафіку, між якими проходить дуже тонка грань. Прості засоби ACL або Black Hole трафіку

влаштовують далеко не всіх. Вихід - використовувати спеціалізовані рішення (комплекси).

Друга лінія оборони – запобігання вторгненням IPS

Використання IPS систем Система запобігання вторгненням (Intrusion Prevention System) — система мережної та комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки та автоматично захищає від них. За рахунок використання технології DPI (Deep Packet Inspection), дані пристрої аналізують трафік 7-го рівня моделі OSI. Системи IPS встановлюватимуться Inline, системи IDS (Intrusion Detection System) підключаються в режимі TAP і отримують копію трафіку без можливості впливати на неї. Методи детектування загроз:

• Signature-Based Detection (перевірка трафіку на основі наявних pattern-он);

• Statistical anomaly-based detection (порівняння штатного трафіку з аномальним);

• Stateful Protocol Analysis Detection (перевірка легітимності заголовків протоколу). Список провідних вендорів згідно з лабораторією NSSLabs.

Третя лінія оборони – Firewall

Використання Firewall Міжмережевий екран (Firewall) - комплекс апаратних або програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього, відповідно до заданих правил. Основне завдання – захист комп'ютерних мереж чи окремих вузлів від несанкціонованого доступу методом визначення політик. Основними функціями є: Packet Filtering, NAT, VPN, Stateful Packet Inspection. Зараз, часто, використовують Next Generation Firewall до якого на відміну від звичайного Firewall додані такі функції: IPS, Application Security, SSL Inspection, UTM (Antivirus, Antispam, Content filtering). Варто відзначити, що при включенні всього функціоналу IGFW продуктивність пристрою значно падає. Тому необхідно розділяти функції NGFW по різних пристроях.

Оборона доступу – NAC

Використання NAC рішень NAC (Network Access Control) — комплекс технічних засобів та заходів, що забезпечує контроль доступу до мережі на підставі інформації про користувача та стан комп'ютера, що отримує доступ до мережі, зокрема на основі інформації про його програмне забезпечення. NAC забезпечує контроль за тим, до яких ділянок мережі та до яких програм отримає доступ користувач на підставі:

• інформації про користувача, який підключається;

• інформації про стан комп'ютера (встановлене програмне забезпечення, наявність оновлень та ін.);

• час підключення;

• точки підключення. Правила контролю доступу можуть застосовуватись за допомогою:

• Призначення користувача у VLAN (802.1x); • Застосування ACL;

• Обмежень пропускної спроможності.

Захист від витоку зсередини - DLP

Використання DLP Запобігання витоку (Data Leak Prevention, DLP) — технології запобігання витоку конфіденційної інформації з інформаційної системи зовні. DLP-системи будуються на аналізі потоків даних, що перетинають периметр інформаційної системи, що захищається. Основні функції DLP-систем

• контроль передачі інформації через Інтернет за допомогою E-Mail, HTTP, HTTPS, FTP, Skype, ICQ та інших додатків та протоколів;

• контроль збереження інформації на зовнішні носії – CD, DVD, flash, мобільні телефони тощо;

• захист інформації від витоку шляхом контролю виведення даних на друк;

• блокування спроб пересилання/збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти, створення тіньових копій, використання карантинної папки;

• пошук конфіденційної інформації на робочих станціях та файлових серверах за ключовими словами, мітками документів, атрибутами файлів та цифровими відбитками.

Захист мобільних користувачів все більш популярним стає робота на мобільних пристроях або робота вдома. Такий підхід до праці називається BYOD (Bring Your Own Device).

MDM - управління мобільними пристроями Управління мобільними пристроями (Mobile device management, MDM) — набір сервісів та технологій, що забезпечують контроль та захист мобільних пристроїв (планшет, телефон), що використовуються організацією та її співробітниками. Корпоративні дані користувача оброблятимуться в окремому «контейнері» (області) на пристрої.

Переваги:

• Роздільне зберігання корпоративних та особистих додатків та даних

• Захист додатків та даних у контейнерах

• Запобігання доступу колишніх працівників до програм та даних

• Безпечний браузер

• Бекап, перепрошивка

• Блокування втраченого пристрою.

Шифроване підключення SSL VPN SSL VPN - Організація віддаленого доступу Virtual Private Network за допомогою використання Secure Sockets Layer криптографічного протоколу. Переваги SSL VPN перед іншими технологіями (IPSec):

• Досить лише браузера щоб отримати доступ до ресурсу по захищеному каналу;

• Платформо-незалежний доступ;

• Не має значення чи ви за NAT-ом, чи у вас закриті всі порти.

Фільтрування WEB та поштового трафіку Web Application Firewall (WAF) – має розширені можливості аналізу та фільтрації WEB-трафіку. Використовує сигнатуру, евристику, двосторонній контроль трафіку. Захищає від: cross-site scripting, SQL injection, buffer overflows, file inclusion, denial of

service, cookie poisoning, schema poisoning. WEB та поштова фільтрація здатні в онлайн режимі проводити сканування запитуваних ресурсів та отриманих листів на предмет вкладених загроз, спаму. За допомогою глобальних (хмарних) служб збору інформації дані системи можуть виконувати репутаційну фільтрацію. Також, за допомогою WEB фільтрації на NGFW можна гнучко керувати доступом користувачів до ресурсів Інтернету, виконувати фільтрацію за категоріями (соціальні мережі, новини, пошук роботи тощо).

Засноване на емуляції виявлення - метод виявлення ще невідомих шкідливих програм шляхом моделювання їх поведінки у пісочниці. Пісочниця (sandbox) — спеціально виділене середовище (найчастіше віртуальне) для безпечного виконання комп'ютерних програм. Як правило, пісочниці використовують для запуску неперевіреного коду з невідомих джерел як засіб проактивного захисту від шкідливого коду, а також для виявлення та аналізу шкідливих програм. Більшість NGFW мають вбудовані пісочниці або пісочниці в хмарі. Також існують окремі рішення.

Використання SIEM (Security information and event management) – об'єднання двох термінів, що позначають область застосування ПЗ: SIM – Security information management – управління інформаційною безпекою та SEM – Security event management – управління подіями безпеки. Технологія SIEM забезпечує аналіз у реальному часі подій (тривог) безпеки, що походять від мережевих пристроїв та додатків. Функції: Агрегація даних, Кореляція, Оповіщення, Засоби відображення, Зберігання даних, Експертний аналіз.

Інвентаризація та аналіз Інвентаризація — складання списку систем, об'єктів, що підлягатимуть захисту та суб'єктів, які задіяні в даному інформаційному просторі, та впливатимуть на інформаційний захист системи. Аналіз захищеності являє собою комплекс робіт з пошуку вразливостей та “слабких” місць у захисті інформаційної системи, а також причин їх виникнення та вироблення рекомендацій щодо їх усунення.

2.3 Сучасний стан нейромереж

На сьогоднішній день накопичені та систематизовані найрізноманітніші підходи щодо застосування статистичних та математичних алгоритмів для побудови систем ШІ, таких як байєсовські методи, логістична регресія, метод опорних векторів, вирішальні дерева, ансамблі алгоритмів тощо [19]. У 2005-2008 роках у дослідженнях з ІІ стався якісний стрибок. Математичний науковий світ почав активно вивчати підхід, заснований на моделі навчання багатошарових нейронних мереж, що стали фундаментом розвитку іншої теорії – глибокого машинного навчання. А ІТ-галузь почала розробляти перші прикладні системи на основі цих підходів та активно вивчати їх.

Останнім часом ряд зарубіжних експертів дійшли висновку, що більшість сучасних і справді вдалих реалізацій – це рішення, побудовані на технології глибоких нейронних мереж (deep neural networks) та глибокого машинного навчання (deep learning) [3].

В даний час існує безліч моделей реалізації нейронних мереж. Є «класичні» одношарові нейронні мережі, вони використовуються для вирішення найпростіших завдань. Одношарова нейронна мережа ідентична в математичному сенсі звичайному поліномі, ваговій функції, що традиційно застосовується в експертних моделях. Число змінних у поліномі дорівнює числу входів мережі, а коефіцієнти перед змінними дорівнюють ваговим коефіцієнтам синапсів.

Є математичні моделі, в яких вихід однієї нейромережі прямує на вхід іншої, і створюються каскади зв'язків, так звані багатошарові нейронні мережі (MNN, multilayer neural network), і один з найбільш розвинених її варіантів, створеного спеціально для розпізнавання образів на зображеннях – згорткові нейронні мережі (CNN, convolutional neural network).

MNN мають великі обчислювальні можливості, але й вимагають великих обчислювальних ресурсів. З урахуванням розміщення ІТ систем у

хмарній інфраструктурі, багатошарові нейромережі стали доступні більшій кількості користувачів. Наприклад, у 2016 році компанія Digital Reasoning із США, що займається когнітивними обчислювальними технологіями, створила та навчила нейронну мережу, що складається із 160 мільярдів цифрових нейронів. Це значно потужніше нейромереж, що є у розпорядженні компаній Google (11,2 мільярда нейронів) та Національної лабораторії США в Ліверморі (15 мільярдів нейронів) [7].

Іншим цікавим різновидом нейромереж є нейронні мережі зі зворотним зв'язком (RNN, recurrent neural network), коли вихід із шару мережі подається назад на один із входів. Такі платформи мають «ефект пам'яті», і вони здатні відстежувати динаміку змін вхідних факторів. Простий приклад – посмішка. Людина починає усміхатися з ледь помітних рухів мімічних м'язів очей та обличчя, перш ніж явно покаже свої емоції. RNN дозволяє виявити такий рух ще на ранніх фазах, що буває корисним для прогнозування поведінки живого об'єкта в часі за допомогою аналізу серії зображень або конструювання послідовного потоку мовлення на природній мові.

Машинне навчання (machine learning) – це процес машинного аналізу підготовлених статистичних даних для пошуку закономірностей та створення на їх основі потрібних алгоритмів (налаштування параметрів нейронної мережі), які потім використовуватимуться для прогнозів.

Розрізняють 3 основні підходи до машинного навчання [25]:

- Навчання з учителем;
- Навчання з підкріпленням;
- Навчання без вчителя (самонавчання).

У навчанні з учителем використовуються спеціально відібрані дані, в яких вже відомі та надійно визначені правильні відповіді, а параметри нейронної мережі підлаштовуються так, щоб мінімізувати помилку. У цьому способі ІІ може зіставити правильні відповіді кожного вхідного прикладу і виявити можливі залежності відповіді від вхідних даних. Наприклад, колекція рентгенологічних знімків із зазначеними висновками буде базою для навчання

ІІ – його «учителем». З серії отриманих моделей людина в результаті вибирає найбільш підходящу, наприклад, за максимальною точністю прогнозів, що видаються.

Нерідко підготовка таких даних та ретроспективних відповідей потребує великого людського втручання та їхнього ручного відбору. Також на якість одержаного результату впливає суб'єктивність людини-експерта. Якщо з будь-яких міркувань він не розглядає при тренуванні всю сукупність вибірки та її атрибутів, його понятійна модель обмежена поточним рівнем розвитку науки і техніки, зазначеною «сліпотою» матиме і отримане ІІ рішення.

Важливо відзначити, що нейромережі є функцією з нелінійними перетвореннями і мають гіперспецифічність - результат роботи алгоритму ШІ буде непередбачуваним, якщо на вхід будуть подані параметри, що виходять за межі значень навчальної вибірки. Тому важливо навчати ШІ систему на прикладах та частотності, адекватних наступним реальним умовам експлуатації. Сильно впливає географічний та соціо-демографічний аспект, що, у загальному випадку, не дозволяє використовувати без втрати точності математичні моделі, натреновані на популяційні дані інших країн та регіонів. За репрезентативність навчальної вибірки також відповідає експерт.

Механізми глибокого машинного навчання (deep learning) використовують, як правило, багатошарові нейромережі та дуже велику кількість екземплярів об'єктів для тренування нейронної мережі. Число записів у навчальній вибірці має налічувати сотні тисяч або навіть мільйони прикладів, а коли ресурси не обмежені – і більше.

Наприклад, для того щоб навчити ІІ розпізнавати обличчя людини на фотографії, команді розробників у Facebook знадобилися мільйони зображень з метаданими та тегами, які говорять про наявність особи на фото. Успіх Facebook у реалізації функції розпізнавання осіб саме лежав у величезній кількості вихідної для навчання інформації: у соціальній мережі є акаунти сотень мільйонів людей, які викладали гігантську кількість фотографій і при цьому вказували на них особи та відзначали (ідентифікували) людей. Глибоке

машинне навчання на основі такої кількості даних дозволило створити надійний штучний інтелект, який тепер за лічені мілісекунди не просто виявляє обличчя людини на зображенні, але й досить часто вгадує, хто саме зображений на фотографії.

Велика кількість записів навчальної вибірки потрібна ІІ та для створення необхідних правил класифікації. Чим більше різнорідних даних буде завантажено в систему на етапі машинного навчання, тим точніше будуть виявлені ці правила, і тим зрештою, точніше буде результат роботи ІІ. Наприклад, при обробці рентгенограм і МРТ багатошарові нейромережі здатні за зображеннями скласти уявлення про анатомію людини та її органи. Водночас придумати у своїй комп'ютерній класифікації назви органів, аналогічні до класичної лікарської термінології, комп'ютери не зможуть. Тому їм спочатку потрібно «перекладач» з внутрішнього машинного словника на професійну лексику. Для підготовки мотивованого судження потрібен людина-експерт, або, як не парадоксально, інша нейромережа, натренована на завдання написання коректних розшифровок і висновків природною людською мовою.

Метод навчання з учителем більш зручний і переважний у тих ситуаціях, коли є накопичені та достовірні ретроспективні вихідні дані: навчання на їх основі вимагатиме менше витрат часу та дозволить швидше отримати працююче ІІ-рішення. Там, де можливість отримати базу даних із зіставленою інформацією та відповідями на неї відсутня – необхідно застосовувати методи самонавчання на основі глибокого машинного навчання; такі рішення не потребуватимуть нагляду людини.

Нам здається, що дослідникам і стартапам, які тільки починають знайомитися з ІІ та шукають можливості його застосування в охороні здоров'я, доцільно розпочати саме з методів машинного навчання з учителем. Це вимагатиме менше витрат (тимчасових, фінансових) на створення прототипу працюючої системи та практичне освоєння методик ІІ. Функціонуючу систему ІІ під конкретне завдання у разі можна отримати швидше. В даний час на ринку є велика кількість якісних бібліотек програмного коду для штучних

нейромереж, таких як TensorFlow https://www.tensorflow.org/ для математичного моделювання, OpenCV http://opencv.org/ для задач розпізнавання зображень, що поставляються безкоштовно, за ліцензією "вільне програмне забезпечення".

Крім практичного ефекту у підвищеній точності, яка сьогодні може досягати 95%, системи ІІ в момент обробки даних мають високу швидкість роботи. Неодноразово проводилися експерименти, наприклад, розпізнавання образів з різних ракурсів, в яких змагалися людина і комп'ютер. Поки темп показу зображень був невисокий - 1-2 кадри за хвилину, людина безумовно вигравав у машини. При аналізі зображень патології помилка людини становила трохи більше 3,5%, а комп'ютер давав помилку діагностики 7,5%. Однак, при підвищенні темпу до 10 кадрів за хвилину і вище у людини слабшала реакція, наставала стомлюваність, що призводило до шлюбу в роботі. Комп'ютер же безперервно навчався на своїх помилках і в наступній серії лише підвищував точність роботи. Перспективним виявився режим парної роботи людини і комп'ютера, при якому вдалося підвищити точність діагностики на 85% відносно високої для людини швидкості демонстрації зображень [5].

Використання технологій глибокого машинного навчання штучних нейронних мереж виправдано там, де неможливо задати чіткі правила, формули та алгоритми для вирішення завдання. Наприклад, у відповідь питання «чи є на рентгенологічному знімку патологія?». Такий підхід передбачає, що замість створення програм для розрахунку заздалегідь заданих формул, машину навчають за допомогою великої кількості даних та різних методів, які дають можливість самостійно виявити цю формулу на основі емпіричних даних і тим самим навчитися виконувати завдання в майбутньому.

РОЗДІЛ 3
ПЕРЕВАГИ ПРИ ВИКОРИСТАННІ ШТУЧНИХ НЕЙРОМЕРЕЖ В КІБЕРБЕЗПЕЦІ

3.1 Основні принципи навчання нейромереж

Існує думка про те, що нейромережа формується «під завдання». Однак у природі є ідеальна, універсальна, «уніфікована» нейромережа – наш мозок. Кожен нейрон можна вважати своєрідним процесором: він підсумовує з відповідними вагами сигнали, що приходять від інших нейронів, виконує нелінійну (наприклад, порогову) функцію і передає результативне значення пов’язаним з ним нейронам. Відповідно до чинного правила «все або нічого» в найпростіших моделях нейронів вихідний сигнал приймає двійкові значення: 0 або 1. Значення 1 відповідає перевищенню порога збудження нейрона, а значення 0 – збудженню нижче порогового рівня. В одній з перших моделей нейрона, званої моделлю Мак-Каллока-Пітса, запропонованої в 1943, нейрон вважається бінарним елементом. Вхідні сигнали підсумовуються з урахуванням відповідних ваг у суматорі, після чого результат порівнюється з пороговим значенням. Модель Мак-Каллока-Пітса – це дискретна модель, у якій стан нейрона зараз розраховується за значеннями його вхідних сигналів у попередній момент.

При вирішенні завдань ідентифікації та управління динамічними процесами нейронна мережа виконує кілька функцій. Вона являє собою нелінійну модель цього процесу, що забезпечує вироблення відповідного керуючого впливу. Мережа також діє як система стеження, яка адаптується до умов навколишнього середовища, що змінюються. Дуже важливою, особливо під час управління роботами, є функція класифікації, яка реалізується при виробленні рішення щодо подальшого розвитку процесу.

Основний механізм запам’ятовування, реалізований у природі, можна представити таким чином. Імпульс збудження, проходячи через синапс,

«нагрівається» і зменшує його опір, збільшуючи масу синапсу. На наступних етапах, при наступному пред'явленні еталона імпульсу збудження, шлях збудження долається більш впевнено, вказуючи відповідне зображення з більшою визначеністю, а використовувані в цьому процесі синапси, «розігріваючись», зберігають, а можливо, і збільшують вагу. Тут працює відоме правило Хебба: синапсичний вага зв'язку двох збуджених нейронів збільшується.

Таким чином, досягається навіть ефект локалізації та максимізації збудження на вихідному шарі, що дублює, а можливо і усуває необхідність взаємодії сусідніх нейронів.

Відзначимо і важливу роль уяви: зразки на вхідному шарі підтримуються досить довго, відновлюються або моделюються. Мабуть, тут велике значення має епіфіз, «третє око» - орган уяви та медитації, пам'ять і генератор видінь.

Нейронні мережі можуть змінювати свою поведінку залежно від стану навколишнього середовища. Після аналізу вхідних сигналів (можливо, разом з необхідними вихідними сигналами) вони самоналаштовуються і навчаються, щоб забезпечити правильну реакцію. Навчена мережа може бути стійкою до деяких відхилень вхідних даних, що дозволяє їй правильно «бачити» образ, що містить різні перешкоди та спотворення.

Існує велика кількість різних конфігурацій нейронних мереж з різними принципами функціонування, які спрямовані на вирішення найрізноманітніших завдань. Як приклад розглянемо багатошарову повно-пов'язану нейронну мережу прямого поширення, яка широко використовується для пошуку закономірностей та класифікації образів. Пов'язаною нейронною мережею називається багатошарова структура, в якій кожен нейрон довільного шару пов'язаний з усіма нейронами попереднього шару, а у випадку першого шару – з усіма входами нейронної мережі. Пряме поширення сигналу означає, що така нейронна мережа не містить петель.

Здатність до навчання є основною властивістю мозку. Для штучних нейронних мереж під навчанням розуміється процес налаштування архітектури мережі (структури зв’язків між нейронами) і ваг синаптичних зв’язків (що впливають на сигнали коефіцієнтів) для ефективного вирішення поставленої задачі. Зазвичай навчання нейронної мережі складає деякій вибірці. У міру процесу навчання, який відбувається за деяким алгоритмом, мережа повинна все краще і краще (правильніше) реагувати на вхідні сигнали.

Виділяють три парадигми навчання: з учителем, самонавчання та змішана. У першому способі відомі правильні відповіді до кожного вхідного прикладу, а ваги підлаштовуються так, щоб мінімізувати помилку. Навчання без вчителя дозволяє розподілити зразки за категоріями за рахунок розкриття внутрішньої структури та природи даних. При змішаному навчанні комбінуються два вищевикладені підходи.

Існує велика кількість алгоритмів навчання, орієнтованих вирішення різних завдань. Серед них виділяє алгоритм зворотного поширення помилки, який є одним з найбільш успішних сучасних алгоритмів. Його основна ідея у тому, що зміна ваг синапсів відбувається з урахуванням локального градієнта функції помилки. Різниця між реальними та правильними відповідями нейронної мережі, що визначаються на вихідному шарі, поширюється у зворотному напрямку – назустріч потоку сигналів. У результаті кожен нейрон здатний визначити вклад кожної своєї ваги сумарну помилку мережі. Найпростіше правило навчання відповідає методу якнайшвидшого спуску, тобто зміни синаптичних ваг пропорційно їхньому вкладу в загальну помилку.

Звичайно, при такому навчанні нейронної мережі немає впевненості, що вона навчилася найкращим чином, оскільки завжди існує можливість попадання алгоритму в локальний мінімум. Для цього використовуються спеціальні прийоми, що дозволяють вибити знайдене рішення з локального екстремуму. Якщо після кількох таких дій нейронна мережа сходить до того ж рішенню, то можна зробити висновок про те, що знайдене рішення, швидше за все, оптимально.

Штучні нейронні мережі вже використовуються сьогодні в багатьох областях, але, перш ніж вони можуть бути застосовані там, де йдеться про людські життя або значні матеріальні ресурси, необхідно вирішити важливі питання, що стосуються надійності їх роботи. Тому рівень допустимих похибок повинен визначатися виходячи з характеру самої проблеми. Деякі проблеми з аналізом питань надійності виникають через припущення, що комп'ютери повністю безпомилкові, у той час як штучні нейронні мережі можуть бути неточними, навіть якщо вони функціонують правильно. Насправді комп'ютери, як і люди, теж можуть помилятися. Перша – через різні технічні неполадки чи помилки у програмах, друга – через неуважність, втому чи непрофесіоналізм. Тому для особливо важливих завдань необхідно, щоб ці системи дублювали і страхували одна одну. А це означає, що при вирішенні таких завдань нейронні мережі повинні виступати не як єдиний засіб, а як додаткові, що запобігають особливим ситуаціям або беруть під контроль, коли проблема не вирішується стандартним способом і будь-які затримки можуть призвести до катастрофи.

Інша труднощі у використанні нейронних мереж у тому, що традиційні нейронні мережі що неспроможні пояснити, як вирішують цю проблему. Внутрішнє уявлення результатів навчання часто буває настільки складним, що його неможливо проаналізувати, за винятком деяких простих випадків, які зазвичай не цікаві.

Останнім часом активно робляться спроби об'єднати штучні нейронні мережі та експертні системи. У такій системі штучна нейронна мережа може реагувати на більшість відносно простих випадків, а всі інші передаються на експертизу в експертну систему. У результаті складні випадки приймаються на вищому рівні, хоча, можливо, і зі збором додаткових даних або навіть із залученням експертів.

Пакеты прикладных программ для нейронных сетей, разработанные рядом компаний, позволяют пользователям работать с различными типами нейронных сетей и с различными способами их обучения. Они могут быть либо

специали-зированными (например, для прогнозирования цены акций), либо вполне уни-версальными.

Області застосування нейронних мереж дуже різноманітні – це розпізнавання тексту і мови, семантичний пошук, експертні системи та системи підтримки прийняття рішень, передбачення курсів акцій, системи безпеки, аналіз текстів. Розглянемо кілька особливо яскравих і цікавих прикладів використання нейронних мереж у різних областях. Необхідно відзначити, що ми намагалися по можливості вибирати найбільш ранні випадки застосування нейронних мереж при вирішенні відповідного завдання.

Нейронні мережі активно використовуються на фінансових ринках. Наприклад, американський Citibank використовує нейромережні прогнози з 1990 року, і вже за два роки після їх впровадження, за свідченням журналу The Economist, автоматичний дилінг показував прибутковість 25% річних. Chemical Bank застосовує нейромережеву систему фірми Neural Data для попередньої обробки транзакцій на валютних біржах ряду країн, відстежуючи підозрілі угоди. Автоматизовані системи ведення портфелів з використанням нейромереж є на озброєнні і в Deere & Co LBS Capital, причому експертна система об’єднується приблизно з 900 нейронними мережами.

У вересні 1992 року компанія HNC, яка до цього займалася виробництвом нейрокомп’ютерів, випустила програмний продукт Falcon, що дозволяє виявляти і запобігати в реальному часі підозрілі угоди по краденим кредитним і дебетним карткам. Штучні нейронні мережі навчалися типової поведінки клієнтів і могли виявляти різке зміна характеру покупок, що сигналізує про можливу крадіжку. Щорічний збиток великих банків від подібних злочинів вимірювався десятками мільйонів доларів, але завдяки впровадженню Falcon в 1994 році вперше за всю історію пластикових карт ці втрати пішли на спад. Аналогічна система була розроблена фірмою ITC для моніторингу операцій з кредитними картками Visa.

Кілька років тому великий канадський банк CIBC для управління рисами та ідентифікації зловмисників встановив програму KnowledgeSeeker фірми

Angoss. З її допомогою фахівці банку вирішили з’ясувати, хто з їхніх клієнтів у майбутньому буде з високою часткою ймовірності затримувати виплати за заставними. Спочатку передбачалося, що в першу чергу ними виявляться ті, хто й раніше затримував свої виплати на кілька днів. Проте дослідження показали, що у майбутньому проблеми з платежами виникнуть у тих клієнтів банку, які на тлі регулярних виплат іноді нібито забували заплатити. Як з’ясувалося, подібна «забудькуватість» була пов’язана з серйозними фінансовими труднощами.

Таким чином, основний механізм запам’ятовування, реалізований у природі, можна представити наступним чином. Імпульс збудження, проходячи через синапс, нагрівається і зменшує його опір, збільшуючи масу синапсу. На наступних етапах, при наступному пред’явленні еталона імпульсу збудження, шлях збудження долається більш впевнено, вказуючи відповідне зображення з більшою визначеністю, а використовувані в цьому процесі синапси, розігріваючись, зберігають, а можливо, і збільшують вагу.

Отже, досягається навіть ефект локалізації і максимізації збудження на вихідному шарі, що дублює, а можливо і усуває необхідність взаємодії сусідніх нейронів.

3.2 Етапи вирішення задач за допомогою нейромереж

Основні етапи вирішення задач за допомогою нейромереж наступні:

- Збір даних для навчання;
- Підготовка та нормалізація даних;
- Вибір топології мережі;
- Експериментальний підбір параметрів мережі;
- Експериментальний вибір параметрів навчання;
- Власне навчання;
- Перевірка адекватності навчання;
- Коригування параметрів, остаточне навчання;

– Вербалізація мережі для подальшого використання.

Деякі з цих кроків слід розглянути докладніше. Отже, розглянемо для початку перший крок «Збір даних для навчання». Вибір даних для навчання мережі та їх обробка є найскладнішим етапом вирішення задачі. Набір даних для навчання повинен задовольняти декільком критеріям: репрезентативність і несуперечність.

Репрезентативність – дані повинні ілюструвати справжнє становище речей у предметній області, несуперечність – суперечливі дані в навчальній вибірці призведуть до поганої якості навчання мережі.

Вихідні дані перетворюються на форму, в якій вони можуть подаватися на мережеві входи. Кожна запис у файлі даних називається навчальною парою або навчальним вектором. Навчальний вектор містить за одним значенням для кожного входу мережі і, залежно від типу навчання (з викладачем або без нього), по одному значенню для кожного виходу мережі. Навчання мережі на «сирому» наборі, як правило, не дає якісних результатів. Існує цілий ряд способів покращити сприйняття мережі. Перше їх це нормування. Вона виконується, коли на різні входи подаються дані різної розмірності. Наприклад, перший вхід мережі подаються величини зі значеннями від нуля до одиниці, але в другий — від ста до тисячі. За відсутності нормування значення на другому вході завжди будуть істотно більший вплив на вихід мережі, ніж значення на першому вході. При нормуванні розмірності всіх вхідних та вихідних даних зводяться докупи. Наступне – квантування. Воно виконується над безперервними величинами, котрим виділяється кінцевий набір дискретних значень. Наприклад, квантування використовують завдання частот звукових сигналів при розпізнаванні промови. І останнє – фільтрація, виконується для «зашумлених» даних.

Крім того, велику роль грає уявлення як вхідних, так і вихідних даних. Припустимо, що мережа вчиться розпізнавати літери в зображеннях і має один числовий вихід – номер літери в алфавіті. У цьому випадку в мережі виникне хибне уявлення про те, що літери з цифрами 1 і 2 більш схожі, ніж літери з

цифрами 1 і 3, що загалом не так. Щоб уникнути такої ситуації, вони використовують мережеву топологію з великою кількістю виходів, де кожен вихід має власне значення. Чим більше виходів в мережі, тим більша відстань між класами і тим складніше їх переплутати.

Розглянемо наступний крок – вибір топології мережі. Вибір типу мережі повинен ґрунтуватися на постановці задачі та наявних даних для навчання. Для навчання з викладачем по кожному елементу вибірки потрібна “експертна” оцінка. Іноді отримати таку оцінку для великого набору даних просто неможливо.) При вирішенні інших завдань (наприклад, прогнозування часових рядів) експертна оцінка вже міститься у вихідних даних і може бути виділена в процесі їх обробки.У цьому випадку можна використовувати багатошаровий персептрон або словесну мережу.

Наступний крок – експериментальний вибір характеристик мережі. Після вибору конкретної топології необхідно вибрати параметри нейронної мережі. Цей етап особливо важливий для мереж, які навчаються з учителем. Від правильного вибору параметрів залежить не тільки те, наскільки швидко відповіді мережі сходитимуться до правильних відповідей. Наприклад, вибір низької швидкості навчання збільшить час сходження, проте іноді дозволяє уникнути паралічу мережі. Збільшення моменту навчання може призвести як до збільшення, так і до зменшення часу збіжності, залежно від форми поверхні помилки. Виходячи з такого суперечливого впливу параметрів, можна зробити висновок, що їх значення потрібно вибирати експериментально, керуючись при цьому критерієм завершення навчання (наприклад, мінімізація помилки або обмеження за часом навчання).

Далі відбувається навчання мережі. У процесі навчання мережа в певному порядку переглядає навчальну вибірку. Порядок перегляду може бути послідовним, випадковим тощо. Деякі мережі навчання, не пов’язані з викладачами (наприклад, мережі Хопфілда), дивляться на зразок лише один раз. Інші (наприклад, мережі Кохонена), а також мережі, що навчаються з учителем, дивляться на вибірку багато разів, і один повний прохід через вибірку

називається епохою навчання. При навчанні з викладачем набір вхідних даних ділиться на дві частини – власне навчальну вибірку та тестові дані; Принцип поділу може бути довільним. Навчальні дані передаються в мережу для навчання, а перевірочні дані використовуються для обчислення помилки мережі (перевірочні дані ніколи не використовуються для навчання мережі). Таким чином, якщо помилка зменшується на перевірочних даних, мережа дійсно виконує узагальнення. Якщо помилка на навчальних даних продовжує зменшуватися, а помилка на тестових даних збільшується, то мережа перестала узагальнювати і просто запам’ятовує навчальні дані. Це називається мережевою перепідготовкою чи перенавчанням. У разі навчання зазвичай припиняється. У процесі навчання можуть виникнути й інші проблеми, такі як параліч або влучення мережі в локальний мінімум поверхні помилок. Неможливо заздалегідь передбачити прояв тієї чи іншої проблеми, а також дати однозначні рекомендації щодо її вирішення.

Все вищесказане відноситься лише до ітераційних алгоритмів пошуку нейромережевих рішень. Для них дійсно нічого не можна гарантувати та неможливо повністю автоматизувати навчання нейронних мереж. Однак поряд з ітеративними алгоритмами навчання не існує ітеративних алгоритмів, що володіють дуже високою стабільністю і дозволяють повністю автоматизувати процес навчання.

Навіть у разі успішного, на перший погляд, навчання мережа не завжди навчається саме тому, що хотів від неї творець. Тому завжди варто проводити перевірку адекватності навчання. Відомий випадок, коли мережа навчилася розпізнавати зображення танків за фотографіями, але пізніше з’ясувалося, що всі танки були сфотографовані на тому самому тлі. Через війну мережа навчилася розпізнавати цей тип місцевості, а чи не навчилася розпізнавати танки. Таким чином, мережа розуміє не те, що від неї вимагалося, а те, що легше всього узагальнити.

Тестування якості навчання нейронної мережі необхідно проводити на прикладах, які не брали участь у її навчанні. Кількість тестових випадків має

бути тим більшою, чим вища якість навчання. Якщо ймовірність помилок нейронної мережі близька до мільярда, то для підтвердження цієї імовірності необхідний мільярд тестових прикладів. Виявляється, що тестування добре навчених нейронних мереж стає дуже складним завданням.

У галузі управління нейронні системи використовуються в завданнях ідентифікації об’єктів, алгоритмах прогнозування та діагностики, а також для синтезу оптимальних АСР. Для реалізації АСР на основі Анн в даний час інтенсивно розробляється виробництво нейрочіпів та нейроконтролерів.

У певному сенсі штучні нейронні мережі є імітатором мозку, який має здатність вчитися та орієнтуватися в умовах невизначеності. Штучна нейронна мережа подібна до мозку в двох аспектах. Мережа набуває знання в процесі навчання, і для збереження знань нею користуються не самі об’єкти, а їх зв’язки – значення коефіцієнтів міжнейронних зв’язків, звані синаптичними вагами або синаптичними коефіцієнтами.

Процедура навчання штучних нейронних мереж полягає у виявленні синаптичних ваг, що забезпечують їм необхідні трансформаційні властивості. Особливістю штучних нейронних мереж є їх здатність змінювати параметри та структуру у процесі навчання.

3.3 Переваги нейромереж

Розв'язання задач при невідомих закономірностях. Використовуючи здатність навчання на безлічі прикладів, нейронна мережа здатна вирішувати завдання, у яких невідомі закономірності розвитку ситуації та залежності між вхідними та вихідними даними. Традиційні математичні методи та експертні системи в таких випадках пасують.

Стійкість до шумів у вхідних даних. Можливість роботи за наявності великої кількості неінформативних, шумових вхідних сигналів. Немає необхідності робити їх попереднє відсівання, нейронна мережа сама визначить їх малопридатність для вирішення завдання і відкине їх.

Адаптування до змін навколишнього середовища. Нейронні мережі мають здатність адаптуватися до змін навколишнього середовища. Зокрема, нейронні мережі, навчені діяти у певному середовищі, може бути легко переучены до роботи за умов незначних коливань параметрів середовища. Більше того, для роботи в нестаціонарному середовищі (де статистика змінюється з часом) можуть бути створені нейронні мережі, що переучуються в реальному часі. Чим вище адаптивні можливості системи, тим стійкішою буде її робота в нестаціонарному середовищі. У цьому слід зазначити, що адаптивність який завжди веде до стійкості; іноді вона призводить до абсолютно протилежного результату. Наприклад, адаптивна система з параметрами, що швидко змінюються в часі, може також швидко реагувати на сторонні збудження, що спричинить втрату продуктивності. Для того, щоб використовувати всі переваги адаптивності, основні параметри системи повинні бути достатньо стабільними, щоб можна було не враховувати зовнішні перешкоди, і досить гнучкими, щоб забезпечити реакцію на істотні зміни середовища.

Потенційна надвисока швидкодія. Нейронні мережі мають потенційну надвисоку швидкодію за рахунок використання масового паралелізму обробки інформації.

Відмовостійкість при апаратній реалізації нейронної мережі. Нейронні мережі потенційно стійкі до відмови. Це означає, що за несприятливих умов їхня продуктивність падає незначно. Наприклад, якщо пошкоджено якийсь нейрон або його зв'язок, вилучення запам'ятованої інформації не може. Однак, зважаючи на розподілений характер зберігання інформації в нейронній мережі, можна стверджувати, що тільки серйозні пошкодження структури нейронної мережі суттєво вплинуть на її працездатність. Тому зниження якості роботи нейронної мережі відбувається повільно.

Важливо відзначити, що штучна нейронна мережа робить узагальнення автоматично завдяки своїй структурі, а не за допомогою використання «людського інтелекту» у формі спеціально написаних комп'ютерних програм.

Деякі зі штучних нейронних мереж мають здатність видобувати сутність із вхідних сигналів.

Наприклад, мережа може бути навчена на послідовність викривлених версій літери «А». Після відповідного навчання пред'явлення такого спотвореного прикладу призведе до того, що мережа породить букву досконалої форми. У певному сенсі вона навчиться породжувати те, що ніколи не бачила.

Область застосування нейромереж у час постійно розширюється, існує безліч вдалих рішень з допомогою даного підходу. Настільки успішне використання нейромережевих рішень, передусім, обумовлено їх перевагами перед звичайними методами [4,5]:

- Існування швидких алгоритмів навчання, нейронна мережа навіть при сотнях вхідних сигналів і десятках-сотнях тисяч еталонних ситуацій може бути швидко навчена на звичайному комп'ютері;

- можливість роботи за наявності великої кількості неінформативних, шумових вхідних сигналів - попереднього їх відсіву робити не потрібно, нейромережа сама визначить їхню малопридатність для вирішення завдання і може їх явно відкинути;

- можливість роботи з скорельованими незалежними змінними, з різнотипною інформацією - безперервнозначною та дискретнозначною, кількісною та якісною, що часто затрудняє методи статистики;

- нейронна мережа одночасно може вирішувати кілька завдань на єдиному наборі вхідних сигналів – маючи кілька виходів, прогнозувати значення кількох показників;

- алгоритми навчання накладають досить мало вимог на структуру нейронної мережі та властивості її нейронів. Тому за наявності експертних знань або у разі спеціальних вимог можна цілеспрямовано вибирати вид і властивості нейронів та нейромережі, збирати структуру нейронної мережі вручну, з окремих елементів, та задавати для кожного з них потрібні властивості.

Незважаючи на великі можливості, існує ряд недоліків, які все ж таки обмежують застосування нейромережевих технологій. Нейронні мережі дозволяють знайти тільки субоптимальне рішення, і відповідно неприйнятні для завдань, які потребують високої точності.

Функціонуючи за принципом чорної скриньки, вони також не застосовуються у випадку, коли необхідно пояснити причину ухвалення рішення.

Навчена нейромережа видає відповідь за частки секунд, проте відносно висока обчислювальна вартість процесу навчання як за часом, так і за обсягом пам'яті також суттєво обмежує можливості їх використання. І все-таки клас завдань, на вирішення яких ці обмеження не критичні, досить широкий.

Можливості, пропоновані нейронними мережами на даний час дозволять створювати системи захисту інформації нового покоління, тобто такі, які мають деяку частку штучного інтелекту. Певна інтелектуалізація систем кібербезпеки надасть безперечних переваг.

Завдяки одній зі своїх надважливих властивостей, здатності до навчання, нейронні мережі дозволять створювати такі системи захисту, які будуть здатні адаптуватися до властивостей об'єкта, що змінюються в часі, що, безсумнівно, позначиться на рівні захисту від кіберзагроз.

РОЗДІЛ IV. ОХОРОНА ПРАЦІ

Основні поняття терміни та визначення у галузі охорони праці

Однією зі специфічних форм людської діяльності є трудова діяльність, під якою розуміється не лише праця в класичному її розумінні, а будь-яка діяльність (наукова, творча, художня, надання послуг тощо), якщо вона здійснюється в рамках трудового законодавства.

Важкість та напруженість праці є одними з головних характеристик трудового процесу.

Під час виконання людиною трудових обов‘язків на неї діє сукупність фізичних, хімічних, біологічних та соціальних чинників. Ці чинники звуться виробничим середовищем.

Сукупність чинників трудового процесу і виробничого середовища, які впливають на здоров‘я і працездатність людини під час виконування нею трудових обов‘язків складають умови праці.

Під безпекою розуміється стан захищеності особи та суспільства від ризику зазнати шкоди.

Реальне виробництво супроводжується шкідливими та небезпечними чинниками (факторами) і має певний виробничий ризик. Виробничий ризик – це ймовірність ушкодження здоров‘я працівника під час виконання ним трудових обов‘язків, що зумовлена ступенем шкідливості та/або небезпечності умов праці та науково-технічним станом виробництва.

Поділення несприятливих чинників виробничого середовища на шкідливі та небезпечні зумовлене різним характером їх дії на людський організм, тим, що вони потребують різних заходів та засобів для боротьби з ними та профілактики викликаних ними ушкоджень, а також рядом причин організаційного характеру. В той же час між шкідливими та небезпечними виробничими факторами інколи важко провести чітку межу. Один і той же чинник може викликати травму і профзахворювання (наприклад, високий

рівень іонізуючого або теплового випромінювання може викликати опік або навіть призвести до миттєвої смерті, а довготривала дія порівняно невисокого рівня цих же факторів – до хвороби; пилинка, що потрапила в око, спричиняє травму, а пил, що осідає в легенях, – захворювання, що зветься пневмоконіоз). Через це всі несприятливі виробничі чинники часто розглядаються як єдине поняття – небезпечний та шкідливий виробничий фактор (НШВФ).

За своїм походженням та природою дії НШВФ можна поділити на 5 груп: фізичні, хімічні, біологічні, психофізіологічні та соціальні.

Один і той же НШВФ за природою своєї дії може належати водночас до різних груп.

Однією з причин появи НШВФ є небезпечні речовини.

Безпека праці – такий стан умов праці, при яких виключена дія на працюючого небезпечних та шкідливих виробничих факторів.

Виходячи з того, що в житті, а тим більше у виробничому процесі, абсолютної безпеки не існує, нерозумно було б вимагати від реального виробництва повного викорінення травматизму, виключення можливості будь-якого захворювання. Але реальним і розумним є ставити питання про зведення до мінімуму впливу об'єктивно існуючих виробничих небезпек. Цю задачу вирішує охорона праці – система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини в процесі трудової діяльності.

Структурно до модулю „Охорона праці” входять наступні складові частини:

правові та організаційні основи;

фізіологія, гігієна праці та виробнича санітарія;

виробнича безпека;

пожежна безпека на виробництві.

Правові та організаційні основи охорони праці являють собою комплекс взаємозв’язаних законів та нормативно-правових актів, соціально-економічних

та організаційних заходів, спрямованих на правильну і безпечну організацію праці, забезпечення працюючих засобами захисту, компенсацію за важку роботу та роботу в шкідливих умовах, навченість працівників безпечному веденню робіт, регламентацію відповідальності та відшкодування працюючим шкоди в разі ушкодження їх здоров‘я.

Фізіологія, гігієна праці та виробнича санітарія – комплекс організаційних, гігієнічних і санітарно-технічних заходів та засобів, спрямованих на запобігання або зменшення дії на працюючих шкідливих виробничих факторів.

Виробнича безпека – безпека від нещасних випадків та аварій на виробничих об‘єктах і від їх наслідків.

Пожежна безпека на виробництві - комплекс заходів та засобів, спрямованих на запобігання запалювань, пожеж та вибухів у виробничому середовищі, а також на зменшення негативної дії небезпечних та шкідливих факторів, які утворюються в разі їх виникнення.

Законодавство України у галузі охорони праці

Законодавство України про охорону праці являє собою систему взаємозв'язаних нормативно-правових актів, що регулюють відносини у галузі реалізації державної політики щодо правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. Воно складається з Закону України «Про охорону праці», Кодексу законів про працю України, Закону України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності" та прийнятих відповідно до них нормативно-правових актів.

Базується законодавство України про охорону праці на конституційному праві всіх громадян України на належні, безпечні і здорові умови праці, гарантовані статтею 43 Конституції України.

Інші статті Конституції встановлюють право громадян на соціальний захист, що включає право забезпечення їх у разі повної, часткової або

тимчасової втрати працездатності (ст. 46); охорону здоров’я, медичну допомогу та медичне страхування (ст. 49); право знати свої права та обов’язки (ст. 57) та інші загальні права громадян, в тому числі, право на охорону праці.

Основоположним документом в галузі охорони праці є Закон України «Про охорону праці», який визначає основні положення щодо реалізації конституційного права працівників на охорону їх життя і здоров'я у процесі трудової діяльності, на належні, безпечні і здорові умови праці, регулює за участю відповідних державних органів відносини між роботодавцем і працівником з питань безпеки, гігієни праці та виробничого середовища і встановлює єдиний порядок організації охорони праці в Україні. Інші нормативні акти мають відповідати не тільки Конституції та іншим законам України, але, насамперед, цьому Законові.

Відповідно до Конституції України, Закону України «Про охорону праці» та Основ законодавства України про загальнообов'язкове державне соціальне страхування у 1999 р. було прийнято Закон України «Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності». Цей закон визначає правову основу, економічний механізм та організаційну структуру загальнообов'язкового державного соціального страхування громадян від нещасного випадку на виробництві та професійного захворювання, які призвели до втрати працездатності або загибелі застрахованих на виробництві.

Закон України «Про охорону праці» має декілька розділів, а саме:

1. Загальні положення.
2. Гарантії прав громадян на охорону праці.
3. Організація охорони праці на виробництві.
4. Стимулювання охорони праці.
5. Державне управління охороною праці.
6. Державний нагляд і суспільний контроль за охороною праці.
7. Відповідальність працівників за порушення законодавства про охорону праці.

До основних законодавчих актів про охорону праці слід віднести також “Основи законодавства України про охорону здоров‘я”, що регулюють суспільні відносини в цій галузі з метою забезпечення гармонічного розвитку фізичних і духовних сил, високої працездатності і довголітнього активного життя громадян, усунення чинників, які шкідливо впливають на їхнє здоров‘я, попередження і зниження захворюваності, інвалідності та смертності, поліпшення спадкоємності. “Основи законодавства України про охорону здоров‘я” передбачають встановлення єдиних санітарно-гігієнічних вимог до організації виробничих та інших процесів, пов‘язаних з діяльністю людей, а також до якості машин, устаткування, будинків та таких об‘єктів, що можуть шкідливо впливати на здоров‘я людей (ст. 28); вимагають проведення обов‘язкових медичних оглядів осіб певних категорій, в тому числі працівників, зайнятих на роботах із шкідливими та небезпечними умовами праці (ст. 31); закладають правові основи медико-соціальної експертизи втрати працездатності (ст. 69).

Крім вищезазначених законів, правові відносини у сфері охорони праці регулюють інші національні законодавчі акти, міжнародні договори та угоди, до яких Україна приєдналася в установленому порядку, підзаконні нормативні акти: Укази і розпорядження Президента України, рішення Уряду України, нормативні акти міністерств та інших центральних органів державної влади. На сьогодні кілька десятків міжнародних нормативних актів та договорів, до яких приєдналася Україна, а також більше сотні національних законів України безпосередньо стосуються або мають точки перетину із сферою охорони праці.

Нормативні акти з охорони праці підприємств

Власники підприємств, установ, організацій або уповноважені ними органи розробляють на основі нормативно-правових актів і затверджують власні нормативні акти з охорони праці, що діють в межах даного підприємства, установи, організації. Нормативні акти підприємства конкретизують вимоги нормативно-правових актів і не можуть містити вимоги з охорони праці менші або слабкіші ніж ті, що містяться в державних нормах.

До основних нормативних актів підприємства належать:

– положення про систему управління охороною праці на підприємстві;

– положення про службу охорони праці підприємства;

– положення про комісію з питань охорони праці підприємства;

– положення про навчання, інструктаж і перевірку знань працівників з питань охорони праці;

– наказ про порядок атестації робочих місць щодо ‘їх відповідності нормативних актів про охорону праці;

– інструкції з охорони праці для працюючих за професіями і видами робіт;

– інструкції про порядок зварювання і проведення інших вогневих робіт на підприємстві;

– загальнооб’єктові та цехові інструкції про заходи пожежної безпеки;

– наказ про порядок забезпечення працівників підприємства спецодягом, спецвзуттям та іншими засобами індивідуального захисту.

Забезпечення безпеки при експлуатації електроустановок. Захист від несприятливої дії електрики**.**

Дія електричного струму на організм людини і види уражень.

Електричний струм чинить на людину біологічне, теплової і хімічну дію. Біологічне - проявляється в порушенні протікають в організмі біологічних процесів, що супроводжуються роздратуванням (руйнуванням) нервових і інших тканин і опіках, припинення діяльності органів дихання та кровообігу. Теплова дія характеризується нагріванням тканин, кровоносних судин, нервів, серця та інших органів, котрі знаходяться на шляху струму. Механічна дія супроводжується розривом тканин, кровоносних судин внаслідок електродинамічного ефекту. Хімічне - розкладає кров, лімфу, порушує їх фізико-хімічний склад.

3.4.2. Фактори, що визначають небезпеку ураження електричним струмом.

– електричні: напруга, сила, рід струму, його частота, електричний опір людини.

– неелектричні: індивідуальні особливості людини, тривалість дії струму і його шлях через людину.

- стан навколишнього середовища.

Електричний струм найменшої сили, що викликає подразнюючу дію юдиною, називається пороговим відчутним струмом. Це приблизно 1,1 мА для струму частоти 50 Гц, а для постійного струму - 6 мА. При струмі 10-15 мА частотою 50 Гц і постійною в 50-80 мА людина не в змозі розтиснути руку, якої стосується струмоведучої частини. Такий струм називається не відпускаючим пороговим. Струм 80-100 мА для частоти 50 Гц і 300 мА для постійного струму викликає припинення кровообігу і смерть. Цей струм називається фібриляціонни, а мінімальне його значення - пороговим фібріаляційним струмом. Струм понад 100 мА (при частоті 50 Гц) миттєво викликає смерть від зупинки серця. Найбільш небезпечним є змінний струм частотою 20-1000 Гц. Значення несприятливого струму для постійного більше в 3 рази, ніж змінного. Електричний опір тіла людини індивідуально, його значення орієнтовно приймається рівним 1000 Ом. Тривалість дії струму на тіло людини пропорційно тяжкості ураження, гранично допустимі рівні напруг дотику і сили струмів вище відпускають встановлені для шляхів струму від однієї руки до іншої, від руки до ніг ГОСТ 12.1.038.

3.4.3Заходи по забезпеченню електробезпеки.

Основними заходами захисту від ураження електричним струмом є:

– забезпечення недоступності электроведущих частин.

– електричний поділ мережі.

– усунення небезпеки ураження, при появі напруги на корпусах інших частинах електроустаткування, що нормально не знаходяться під напругою за допомогою:

а) захисного заземлення,

б) зануленя,

в) захисного відключення;

– застосування малих напруг;

– захист від небезпеки при переході напруги з вищої сторони на нижчу.

– контроль та профілактика пошкоджень ізоляції.

– компенсація ємнісної складової струму на землю.

– застосування спеціальних електрозахисних засобів.

– організація безпечної експлуатації електроустановок.

Застосування малих напруг: 6-12-24-36-42 ст. обмежується труднощами здійснення протяжної мережі. Область застосування: ручний інструмент, переносні лампи, лампи місцевого освітлення, сигналізація.

Електричне розділення мережі, здійснюється шляхом підключення окремих електроприймачів через розділовий трансформатор. Мета - зменшення ємності і збільшення опору мережі. Захист від небезпеки при переході з вищої сторони на нижчу. Небезпека виникає при пошкодженні ізоляції між обмотками ВН і НН трансформатора. Способи захисту залежать від режиму нейтралі. Мережі до 1 кв год ізольованою нейтраллю: пов'язані з мережами вище 3 кв захищають пробивного запобіжника, встановленого в нейтралі або фазі на стороні НН трансформатора.

Контроль та профілактика пошкоджень ізоляції. З плином часу ізоляція "старі". Тому необхідно регулярно виконувати профілактичні випробування, огляди. У приміщеннях без підвищеної небезпеки 1 раз на 2 роки, у небезпечних приміщеннях 1 раз в півроку перевіряють опір ізоляції. За ПУЗ не менше 0,5 мом/фазу ділянки мережі напругою до 1 кв Існують такі прилади контролю ізоляції ПКІ, РУО, УАКІ. Часто застосовується метод випробування ізоляції підвищений напругою. Захист від випадкового дотику до струмоведучих частин.

– огорожа: - суцільна / до 1 кв / - сітчаста;

– блокування (для електроустановок понад 250 В, в яких часто проводяться ремонтні роботи. Блокування бувають електричні і механічні.

Компенсація ємнісної складової струму замикання на землю. Здійснюється введенням в мережу додаткової індукції ПУЕ наказує компенсацію при струмах замикання на землю: 35кВ-10А, 15 - 20 кВ - 15 А,

10кВ-20А, 6кВ - 30А. Захисне заземлення - навмисне електричне з'єднання з землею металевих неструмопровідними частин. Ефективно тільки у випадку, якщо струм замикання на землю не збільшується зі зменшенням опору заземлення. Область застосування: - мережі до 1000 В змінного струму: 3-х фазні с ізольованою нейтраллю, 1-фазні 2-х проводні ізольовані від землі, постійного струму 2-х проводні ізольовані від землі.

– мережі понад 1кВ змінного і постійного струму з будь-яким режимом землі.

Захисному заземленню підлягає обладнання:

– в приміщеннях з підвищеною небезпекою і особливо небезпечних;

– зовнішніх установках при номінальній напрузі вище 42 В змінного струму і 110 В постійного струму;

– у приміщеннях без підвищеної небезпеки при змінному струмі понад 380 В і постійному струмі більш 440В;

– у всіх вибухонебезпечних приміщеннях.

Заземлювачі бувають природними і штучними, виносні та контурні. На вимогу ПУЕ опір заземлення повинне бути дорівнює або менше 4 см у мережах до 1 кВ або 10 дм якщо сумарна потужність джерел підключення до мережі не більше 100 КвА. В мережах понад 1 Кв і струмами замикання на землю більше 500 А опір заземлення повинне бути дорівнює або менше 0,5 Ом , для мереж понад 1 КВ і струмами замикання менше 500 А допускається опір заземлення рівним або менше 250/ Із але не більше 10 Ом.

3.5 Державний і профспілковий контроль за охороною праці на виробництві

Згідно Закону України «О охороні праці» існують позавідомчі органи нагляду і контролю за дотриманням законодавства про працю і правил охорона праці, до якої відносяться державні органи і інспекції, які в своїй діяльності не залежать від адміністрації піднаглядних підприємств і їх віще посадових органів.

Державний нагляд здійснюють:

Державний комітет України з нагляду за охороною праці

Державний комітет України з ядерної і радіаційної безпеки

Органи Державного пожежного нагляду управління пожежної охорони

Органи і установи санітарно-епідеміологічної служби Міністерства охорони здоров'я України.

Вищий нагляд за дотриманням і правильним застосуванням закону про охорону праці здійснюється Генеральним прокурором і підлеглими йому службами. Органи державного нагляду за охороною праці не залежать від яких би те ні було господарських органів, об'єднань громадян, політичних формувань, місцевої державної адміністрації і Рад, і діють відповідно до положень, затверджених кабінетом Міністрів України.

Суспільний контроль за дотриманням законодавства про ОП здійснюють трудові колективи через вибраних ними представників професійні союзи в особі своїх виборних органів і представників.

Уповноважені трудових колективів по питаннях охорони праці мають право безперешкодно перевіряти на підприємстві виконання вимог по охороні праці і вносити обов'язкові для розгляду власником підприємства пропозиції про усунення виявлених порушень нормативних актів по безпеці і гігієні праці. Для виконання цих обов'язків власник за свій рахунок організовує навчання і звільняє уповноваженого по питаннях ВІД від роботи на передбачений колективним договором термін із збереженням за ним середнього заробітку.

Уповноважені трудових колективів діють відповідно до типового положенням, затвердженим Державним комітетом України з нагляду за охороною праці за узгодженням з профспілкою.

Відповідальність за порушення законодавства про охорону праці

Закон України “Про охорону праці” передбачає, що за порушення законів та інших нормативно-правових актів про охорону праці, створення перешкод у діяльності посадових осіб органів державного нагляду за охороною праці, а також представників профспілок, їх організацій та об'єднань винні особи

притягаються до дисциплінарної, адміністративної, матеріальної та кримінальної відповідальності.

Дисциплінарна відповідальність полягає в тому, що на винного працівника накладається дисциплінарне стягнення. Ст. 147 КЗпПУ встановлює два види дисциплінарного стягнення: догана та звільнення з роботи. Законами, уставами та положеннями про дисципліну, які діють в деяких галузях (транспорт, гірничодобувна промисловість тощо), можуть бути передбачені для окремих категорій працівників інші дисциплінарні стягнення.

Адміністративна відповідальність настає за будь-які посягання на загальні умови праці. Відповідно до ст. 41 Кодексу України про адміністративні правопорушення порушення вимог законів та нормативно-правових актів з охорони праці тягне за собою адміністративну відповідальність у вигляді накладання штрафу на працівників та, зокрема, посадових осіб підприємств, установ, організацій, а також громадян – власників підприємств чи уповноважених ними осіб.

Матеріальна відповідальність робітників і службовців регламентується КЗпПУ та іншими нормативними актами, які торкаються цієї відповідальності у трудових відносинах.

Загальними підставами накладення матеріальної відповідальності на працівника є

– наявність прямої дійсної шкоди,

– провина працівника (у формі наміру чи необережності),

– протиправні дії (бездіяльність) працівника,

– наявність причинного зв'язку між винуватим та протиправними діями (бездіяльністю) працівника та заподіяною шкодою.

На працівника може бути накладена відповідальність лише при наявності всіх перелічених умов; відсутність хоча б однієї з них виключає матеріальну відповідальність працівника.

Притягнення працівника до кримінальної, адміністративної і дисциплінарної відповідальності за дії, якими нанесена шкода, не звільнює його від матеріальної відповідальності.

При наявності в діях працівника, яким порушені правила охорони праці, ознак кримінального злочину, на нього може бути покладена повна матеріальна відповідальність, а при відсутності таких ознак на нього покладається відповідальність в межах його середнього місячного заробітку.

Кримінальна відповідальність за порушення правил охорони праці передбачена ст.ст. 271 – 275 КК України, що об‘єднані в розділ Х “Злочини проти безпеки виробництва”.

Кримінальна відповідальність настає не за будь-яке порушення, а за порушення вимог законів та інших нормативно-правових актів про охорону праці, якщо це порушення створило загрозу загибелі людей чи настання інших тяжких наслідків або заподіяло шкоду здоров'ю потерпілого чи спричинило загибель людей або інші тяжкі наслідки.

Порушення вимог законодавчих та інших нормативно-правових актів, передбачених вищезазначеними статтями КК України, карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на строк до п‘яти років, або позбавленням волі на строк до дванадцяти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

ВИСНОВКИ

Таким чином, можна констатувати, що дана тема широко висвітлена у науковій літературі, є безліч публікацій як фундаментальних, так і прикладного характеру. На даний момент основними напрямками, в яких використовуються ШНМ, є медицина, правоохоронна діяльність, держуправління, прогнозування погоди та біржових котирувань, а також незаконна діяльність хакерських груп з метою одержання вигоди. Незважаючи на справді високі фінансові витрати, використання ШНМ з метою захисту інформації бачиться вкрай перспективним з огляду на те, що порушники вже роблять це. У статті автор вносить уточнення до визначення ШНМ, що більш повно розкриває сенс поняття на даний момент часу.

З вище сказаного стає очевидним необхідність розвитку та застосування ШНМ з метою захисту інформації. Можливо, роль людини поступово зменшуватиметься, а машини ставатимуть все більш самостійними. Но сьогодні без участі оператора тандем працювати не може.

Щодо ефективності, то до якихось радикальних змін у боротьбі зі злочинцями технології штучного інтелекту поки що наводять, але в середньостроковій та довгостроковій перспективі прогрес піде саме цим шляхом – стежити за ІТ-системами ІТ-системи. У виграші виявляться ті структури, ті організації, ті країни, які першими почали використовувати такі підходи.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Расходы на кибербезопасность в мире будут расти на 10,6% в год // Daily Comm коммуникации в ИТ-бизнесе. [Электрон. ресурс]. URL: http://www.dailycomm.ru/m/46489/

2. McCulloch W.S. and Pitts W. A logical calculus of the ideas immanent in nervous activity// Bull. Math. Biophys. – №5. – 1943 – p. 115–133.

3. Wiener N. Cybernetics or control and communication in the animal and the machine. – Cambridge Mass. M.I.T. Press: 1962 – 242 p.

4. Петров А.П. О возможностях перцептрона // Известия АН СССР, Техническая кибернетика. – 1964. – № 6. – с. 25 – 57.

5. Бонгард М.М. Проблемы узнавания. – М.: Физматгиз, 1967 – 321 с. 6. Галушкин А.И. Нейронные сети // Большая российская энциклопедия. [Электрон. ресурс]. URL: https://bigenc.ru/technology_and_technique/text/4114009

7. Security intelligence – Overview // IBM. [Электрон. ресурс]. URL: https://www.ibm.com/uken/security/security-intelligence

8. Attacks, Challenges, and New Designs in Security and Privacy // Hindawi. [Электрон. ресурс]. URL: https://www.hindawi.com/journals/wcmc/2020/8859489/

9. National security agency cybersecurity report // NSA. [Электрон. ресурс]. URL: https://media.defense.gov/2019/Jul/16/2002158108/-1/-1/0/CTR_NSA-CSS-TECHNICAL-CYBERTHREAT-FRAMEWORK_V2.PDF

10. Рейтер: массовая хакерская атака привела к заражению продуктов Microsoft // РИА новости. [Электрон. ресурс]. URL: https://ria.ru/20201218/microsoft-1589821871.html

11. Major cyber spy network uncovered // News BBC. [Электрон. ресурс]. URL: http://news.bbc.co.uk/2/hi/americas/7970471.stm

12. Анатомия таргетированной атаки // Kaspersky daily. [Электрон. ресурс]. URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/

13. WannaCry|WannaDecrypt0r NSACyberweapon-Powered Ransomware Worm // GitHub Gist. [Электрон. ресурс]. URL: https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168

14. Russian SVR Targets U.S. and Allied Networks // Cybersecurity Advisory. [Электрон. ресурс]. URL: https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

15. US military defense systems. The anatomy of cyber espionage by Chinese hackers // Georgetown university. [Электрон. ресурс]. URL: http://journal.georgetown.edu/u-s-military-defense-systems-theanatomy-of-cyber-espionage-by-chinese-hackers/

16. Нейронні мережі. Особливості побудови // Neuro.net. [Электрон. ресурс]. URL: http://neuro.net.ua/pub/mcculloch.html

17. Nils Nilsson J. Artificial Intelligence: A New Synthesis/ J. Nils Nilsson // Elsevier Inc. – 1998. – 513 с.

18. T. Mitchell. Machine Learning. A Guide to Current Research/ Tom M. Mitchell, Jaime G. Carbonell, Ryszard S. Michalski (Eds.)// Springer Science & Business Media. – 1986. – 429 с.

19. J. Grus. Data Science from Scratch: First Principles with Python/ Grus J.// O'Reilly Media. – 2015. – 330 с.

20. L. Deng, D. Yu. Deep Learning: Methods and Applications. Foundations andTrends in Signal Processing. – vol. 7. – nos. 3–4. – 2014. – с. 199- 200.

21. Businesses recognize the need for AI & ML tools in cybersecurity// Helpnetsecurity [Электрон. ресурс]. URL: https://www.helpnetsecurity.com/2019/03/14/ai-ml-toolscybersecurity/

22. E. Kaspersky. Laziness, Cybersecurity, and Machine Learning// Kaspersky [Электрон. ресурс]. URL: https://eugene.kaspersky.com/2016/09/26/laziness-cybersecurity-and-machine-learning/

23. J. Roberts. Cyber-Hunting at Scale (CHASE)// DARPA [Электрон.

ресурс]. URL: https://www.darpa.mil/program/cyber-hunting-at-scale

24. Caliskan, F. Yamaguchi, E. Dauber, R. Harang, K. Rieck, R. Greenstadt, A. Narayanan. When Coding Style Survives Compilation: De-anonymizing Programmers from Executable Binaries. arXiv:1512.08546// Arxiv [Электрон. ресурс]. URL: https://arxiv.org/abs/1512.08546

25. Reznik D. Artificial neural networks. analysis of possibilities of use in purposes to ensure information security, 50-54 p.//VOL 1, No 67 (67) (2021), The scientific heritage (Budapest, Hungary)

26. Sternberg R. J. Giftedness According to the Theory of Successful Intelligence. In N. Colangelo & G. Davis (Eds.), Handbook of Gifted Education (88-99). Boston MA: Allyn and Bacon, 2003

27. Бугаков, С. С. Перспективы внедрения нейронных сетей в реализацию систем поддержки принятия решений // Молодой ученый, Москва, 2016, № 4 (108).

28. Крючин О. В., Вязовова Е. В. Перспективы использования информационных систем, базирующихся на технологии искусственных нейронных сетей в различных сферах // Вестник ТГУ – Томск, 2014, №19 (2).

29. Галушкин А.И. Теория нейронных сетей. Серия «Нейрокомпьютеры и их применение». Книга 1. // ИПРЖР, Москва, 2000.