

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки, факультет радіоелектроніки та
телекомунікацій
(повне найменування інституту / факультету)

Кафедра «Захисту інформації»
(повне найменування кафедри)

Пояснювальна записка

до магістерської роботи
(ступінь вищої освіти)

на тему «Забезпечення безпеки інформаційних систем від несанкціонованого
доступу на основі капсульного методу»

Виконала: студентка 2 курсу, групи РТ-819м

Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем
Матвейчук О.В.

(прізвище та ініціали)

Керівник Воскобойник В.О.

(прізвище та ініціали)

Рецензент Фурманова Н.І.

(прізвище та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Інститут, факультет Інститут інформатики та радіоелектроніки, Факультет
радіоелектроніки та телекомунікацій
Кафедра захисту інформації
Ступінь вищої освіти магістр
Спеціальність 125 – «Кібербезпека»

(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних
систем

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри Карпуков Л.М.,
докт. техн. наук, професор

« 01 » 09 2020 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТКИ

Матвейчук Олени Валеріївни

(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) Забезпечення безпеки інформаційних систем від
несанкціонованого доступу на основі капсульного методу
керівник проєкту (роботи) Воскобойник Володимир Олександрович, канд. техн.
наук, доцент, професор кафедри захисту інформації

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

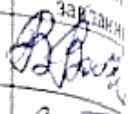
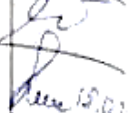
затверджені наказом закладу вищої освіти від «06» листопада 2020 року №314

2. Строк подання студентом проєкту (роботи) 15 грудня 2020 року

3. Вихідні дані до проєкту (роботи) Несанкціонований доступ, захист від
несанкціонованого доступу, інформаційні системи, штучні нейронні мережі,
згорткові нейронні мережі, капсульні нейронні мережі

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно
розробити) Класифікація видів і методів НСД та аналіз методів захисту від
НСД; методи ШНМ для захисту від НСД та аналіз їх недоліків; аналіз
капсульного методу; розробка методики використання КНМ в задачах захисту
ІС від НСД; економічне обґрунтування технічної частини; охорона праці та
безпека в надзвичайних ситуаціях.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
8 рисунків; 13 таблиць; презентація магістерської роботи.

6. Консультанти розділів проєкту (роботи)		Підпис, дата	
Розділ	Прізвище, ініціали та посада консультанта	завдання видав	прийняв виконав завдання
Основні розділи	Воскобойник В.О., доцент, професор	01.09	
Розділ з ОП і НС	Якімцов Ю.В., доцент	10.09	
Розділ з економіки	Круглікова В.В., доцент	10.09	
Нормоконтроль	Корольков Р.Ю., ст. викладач	11.12	

7. Дата видачі завдання «01» вересня 2020 року.

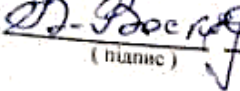
КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Складання та затвердження ТЗ	01.09-14.09	Виконано
2	Підбір літератури	15.09-21.09	Виконано
3	Огляд видів і методів НСД та аналіз методів захисту від НСД	22.09-30.09	Виконано
4	Розгляд методів ШНМ для захисту від НСД та аналіз їх недоліків	01.10-11.10	Виконано
5	Огляд ЗНМ та її недоліків	12.10-14.10	Виконано
6	Аналіз капсульного методу	15.10-23.10	Виконано
7	Розгляд структури, обчислювальних етапів капсули та архітектури КНМ	23.10-29.11	Виконано
8	Огляд методів використання КНМ в задачах захисту ІС від НСД	29.11-2.11	Виконано
9	Розробка методики використання КНМ для розпізнавання об'єктів систем кібербезпеки	02.11-07.11	Виконано
10	Розробка методики використання у ОПМ та аналізі тексту для розпізнавання кіберзагроз	07.11-15.11	Виконано
11	Розробка методики використання у класифікації типів шкідливого ПЗ та можливі напрями розвитку	16.11-25.11	Виконано
12	Розрахунок економічного обґрунтування технічної частини	26.11-01.12	Виконано
13	Розгляд питань з охорони праці та безпеки в надзвичайних ситуаціях	01.12-05.12	Виконано
14	Оформлення пояснювальної записки	07.12-8.12	Виконано
15	Оформлення графічної частини	8.12-10.12	Виконано

Студентка

Керівник проєкту (роботи)

 Матвейчук О.В.
(прізвище та ініціали)

 Воскобойник В.О.
(прізвище та ініціали)

РЕФЕРАТ

ПЗ: 99 сторінок, 8 рисунків, 13 таблиць, 33 джерела.

Об'єкт дослідження – інформаційні системи (ІС), несанкціонований доступ (НСД), методи захисту від НСД, штучні нейронні мережі (ШНМ), згорткові нейронні мережі (ЗНМ), капсульні нейронні мережі (КНМ).

Мета роботи - аналіз існуючих методів захисту ІС від НСД і використання ШНМ для забезпечення кібербезпеки. Дослідження ЗНМ та КНМ для розробки методики їх використання у задачах кіберзахисту.

У першому розділі магістерської роботи проведено аналіз видів і методів НСД, та методів захисту від них.

У другому розділі описані ШНМ та їх використання для захисту від НСД, розглянуті ЗНМ, їх недоліки та можливість використання у задачах захисту від НСД.

У третьому розділі проводиться дослідження капсульного методу: концепція, структура та обчислювальні етапи капсули, динамічна маршрутизація між капсулами та архітектура КНМ.

У четвертому розділі викладена розроблена методика використання капсульного методу для задач кіберзахисту, таких як: розпізнавання об'єктів на зображеннях, відео, тексту та використання в ОПМ для розпізнавання кіберзагроз, класифікації типів шкідливого ПЗ та запропоновані можливі напрями використання КНМ у захисті ІС від НСД.

Також у роботі проведено економічне обґрунтування розробленої методики та розглянуті питання щодо охорони праці та безпеки у надзвичайних ситуаціях.

ЗАХИСТ ВІД НСД, ЗГОРТКОВІ НЕЙРОННІ МЕРЕЖІ, КАПСУЛЬНІ НЕЙРОННІ МЕРЕЖІ, КІБЕРЗАХИСТ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ШТУЧНІ НЕЙРОННІ МЕРЕЖІ

ЗМІСТ

Перелік скорочень і позначень	7
Вступ.....	8
1. Класифікація видів і методів НСД та аналіз методів захисту від НСД.....	11
1.1 Класифікація видів і методів НСД	11
1.2 Аналіз існуючих видів і методів захисту комп'ютера від НСД	13
1.2.1 Ідентифікація	13
1.2.2 Автентифікація	14
1.2.3 Управління доступом.....	15
1.2.4 Технічні методи.....	18
2. Методи ШНМ для захисту від НСД та аналіз їх недоліків.....	20
2.1. Методи ШНМ для захисту від НСД.....	20
2.1.1 Поняття і класифікація ШНМ.....	20
2.1.2 Застосування ШНМ в захисті від НСД.....	25
2.2. Аналіз недоліків ШНМ.....	25
3. Аналіз капсульного методу	28
3.1 Капсульний метод	28
3.1.1 Концепція капсульного методу	28
3.1.2 Точка зору інваріантності та стійкості до змагальної атаки.....	29
3.2 Структура та обчислювальні етапи капсули	31
3.2.1 Порівняння капсули зі штучними нейронами.....	31
3.2.2 Обчислювальні етапи капсули.....	32
3.3 Динамічна маршрутизація між капсулами	35
3.4 Архітектура КНМ.....	37
3.4.1 Кодер	38
3.4.2 Декодер.....	42
4. Розробка методики використання КНМ в задачах захисту ІС від НСД.....	45

4.1 Використання КНМ для розпізнавання об'єктів систем кібербезпеки	45
4.1.1 Використання КНМ для розпізнавання об'єктів чи осіб на зображеннях та відео.....	45
4.1.2 Використання КНМ у виявленні презентаційних атак в біометричних системах автентифікації	46
4.1.3 Використання КНМ у виявленні людських дій на відео	47
4.2 Використання у ОПМ та аналізі тексту для розпізнавання кіберзагроз	49
4.2.1 Використання у ОПМ та аналізі тексту	49
4.2.2 Розпізнавання кіберзагроз.....	51
4.3 Класифікація типів шкідливого ПЗ.....	52
4.4 Можливі напрями розвитку	54
5. Економічне обґрунтування технічної частини.....	58
5.1 Аналіз маркетингової частини проєкту забезпечення безпеки ІС від НСД на основі капсульного методу.....	58
5.2 Визначення витрат на аналіз капсульного методу для забезпечення безпеки ІС від НСД	69
6. Охорона праці та безпека в надзвичайних ситуаціях.....	77
6.1 Аналіз потенційних небезпек	77
6.2 Заходи по забезпеченню техніки безпеки	78
6.3 Заходи з виробничої санітарії та гігієни праці.....	81
6.4 Заходи безпеки у надзвичайних ситуаціях.....	87
6.4.1 Заходи з пожежної безпеки	87
6.4.2 Заходи з цивільного захисту	89
Висновки	92
Перелік використаних джерел	95

ПЕРЕЛІК СКОРОЧЕНЬ І ПОЗНАЧЕНЬ

ЗНМ - згорткова нейронна мережа

ІС - інформаційна система

КНМ – капсульна нейронна мережа

НСД - несанкціонований доступ

ОПМ – обробка природної мови

ПЕМВН - побічне електромагнітне випромінювання і наведення

ПЗ – програмне забезпечення

ПК - персональний комп'ютер

ШНМ - штучна нейронна мережа

ШПЗ – шкідливе програмне забезпечення

ВСТУП

Інформаційні технології – це невід’ємна частина життя людини у сучасному світі, а також - величезна частина ведення бізнесу, тому управління корпоративними даними та даними клієнтів є головним пріоритетом багатьох компаній. Оскільки ця тенденція триватиме, потреба у дослідженні даних буде ставати ще більш важливою.

Бізнес-фірми та інші організації покладаються на ІС для здійснення та управління їх діяльністю, взаємодії зі своїми клієнтами та постачальниками, а також - конкуренції на ринку. ІС використовуються для управління міжорганізаційними ланцюгами поставок та електронними ринками. Наприклад, корпорації використовують ІС для обробки фінансових рахунків, управління своїми людськими ресурсами та охоплення своїх потенційних клієнтів за допомогою онлайн-акцій. Багато великих компаній повністю побудовані навколо ІС. Цифрові товари, такі як електронні книги, відеопродукція та ПЗ, онлайн-послуги, такі як ігри чи соціальні мережі, постачаються з ІС. Люди проводять значну частину свого особистого життя в ІС: для спілкування, навчання, покупок, банківської справи та розваг.

Оскільки інформаційні системи зробили можливою більш різноманітну людську діяльність, вони зробили глибокий вплив на суспільство. Ці системи пришвидшили темп повсякденної діяльності, дозволили людям розвивати та підтримувати нові та часто більш корисні стосунки, впливали на структуру та поєднання організацій, змінювали тип закупуваних продуктів та впливали на характер роботи. Інформація та знання стали життєво важливими економічними ресурсами. Проте разом із новими можливостями залежність від інформаційних систем несла нові загрози. Частота несанкціонованих дій щодо ІС у процесі їх інтеграції неухильно зростає, що неминуче призводить до величезних фінансових та матеріальних втрат. Тому забезпечення

інформаційної безпеки в ІС - це гарантія задоволення законних прав та інтересів суб'єктів інформаційних відносин.

Людство дуже швидко рухається у напрямку штучного інтелекту, який веде до нової інформаційної революції, що можна співставити з масштабами розвитком глобальної мережі Інтернет. Штучний інтелект дуже активно вивчається та набирає обертів. Саме у цій галузі сконцентрована велика кількість високо фахових спеціалістів з програмування, інженерії, математики, лінгвістики і спеціалістів з кібербезпеки. Цими фахівцями розглядаються окремі питання, що пов'язані з розвитком наукової думки, обчислювальної техніки та робототехніки. Через це розробляються нові методи наукового дослідження, через що формуються нові погляди на наукові досягнення та результати, що також впливає і на філософське осмислення отриманих результатів.

ШНМ - це одне з сучасних і перспективних напрямків в різних сферах діяльності, зокрема, в кіберзахисті. Методи ШНМ дають можливість створити нові алгоритми захисту ІС від НСД шляхом використання їх для обслуговування засобів управління ідентифікацією, автентифікацією і доступом до ресурсів, а також засобів адміністрування доступу, оптимізації процесу пошуку шкідливих джерел та ПЗ і їх класифікації, використання в засобах виявлення атак, в брандмауерах та криптографії. Архітектура ЗНМ є найбільш придатною для розпізнавання зображень і їх класифікації. Також, ЗНМ використовуються у відеоаналізі, обробці природної мови, можуть бути використані для аналізу документів та текстів. З її допомогою можливо розпаралелювання обчислень, і, як наслідок, використання графічних процесорів.

Але у ЗНМ є недоліки, задля вирішення яких використовуються капсульні нейронні мережі. Це вкрай перспективна архітектура нейронних мереж для вирішення задачі класифікації, яка не тільки покращує розпізнавання зображень при змінених ракурсах і ієрархічною структурою, але і може

використовувати ці властивості для розпізнавання тексту та використання в ОПМ задля виявлення кіберзагроз та класифікація типів шкідливого ПЗ.

Метою даної роботи є аналіз існуючих методів захисту ІС від НСД і використання ШНМ для забезпечення кібербезпеки. Дослідження ЗНМ та КНМ для розробки методики їх використання у задачах кіберзахисту.

Виходячи з вищевикладеного в даній роботі будуть розглянуті такі питання, як:

- поняття і класифікація видів і методів НСД, а також аналіз існуючих методів захисту;
- аналіз ШНМ, та методів ШНМ для захисту ІС від НСД, аналіз ЗНМ, їх переваг та недоліків;
- аналіз капсульного методу, а саме: його концепція, структура та обчислювальні етапи капсули, динамічна маршрутизація між капсулами, і архітектура КНМ;
- розробка методики використання капсульного методу для задач кіберзахисту, таких як: розпізнавання об'єктів на зображеннях та відео, розпізнавання тексту та використання в ОПМ, розпізнавання кіберзагроз та класифікація типів шкідливого ПЗ. Також були запропоновані можливі напрями використання КНМ у захисті ІС від НСД.

1 КЛАСИФІКАЦІЯ ВИДІВ І МЕТОДІВ НСД ТА АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД НСД

1.1 Класифікація видів і методів НСД

Несанкціонований доступ (НСД) - отримання захищеної інформації зацікавленим суб'єктом з порушенням встановлених правовими документами чи власником інформації прав або правил доступу до захищеної інформації. При цьому зацікавленим суб'єктом, що здійснює НСД до інформації, може бути держава, юридична особа, група фізичних осіб, в тому числі, громадська організація, окрема фізична особа [1].

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [2].

Види НСД. За характером появи їх можна розділити на два види: навмисні та ненавмисні. Ненавмисні загрози - це випадкові дії, які проявляються в недостатній підтримці механізмів захисту або в помилках управління. А навмисні - це несанкціоноване отримання інформації і маніпуляція даними, ресурсами або системами.

В залежності від типу реалізації загрози можуть бути розділені на програмні та технічні. До першої групи відносять ті, які реалізовані у вигляді окремого програмного модуля або модуля в складі програмного забезпечення. До другої групи належать зловживання, засновані на використанні технічних засобів інформаційної системи для підготовки і здійснення комп'ютерних злочинів (наприклад, несанкціоноване підключення до мереж зв'язку, знімання інформації за допомогою спеціальної апаратури та ін.). Кібер-зловмисники служать багатьом цілям і використовують широкий спектр програмних засобів.

Таким чином, можна з'єднати програмні засоби у 2 групи: тактичні та стратегічні. Тактичні – такі, що переслідують досягнення найближчої мети, як наприклад, отримання пароля чи знищення даних або інше. Вони зазвичай використовуються для підготовки та реалізації стратегічних засобів, які спрямовані на реалізацію довгострокової мети, а також пов'язані з великими фінансовими втратами для ІС. До групи стратегічних інструментів входить впровадження, що дозволяє контролювати технологічними процеси перетворення інформації і вплив на роботи компонентів в ІС.

Основні методи несанкціонованого доступу до комп'ютерної інформації діляться на агентурні і технічні (в тому числі і апаратні).

Агентурні:

- психологічний (ініціативне співробітництво; підкуп; співпраця під загрозою);
- пряме підслуховування;
- візуальне знімання.

Технічні:

- подолання програмних засобів захисту;
- несанкціоноване копіювання інформації; перехоплення інформації в каналах зв'язку;
- впровадження програмних закладок і комп'ютерних вірусів;
- використання апаратних закладок;
- перехоплення ПЕМВН, а також деякі інші.

Природно, що такий розподіл є в значній мірі умовним, так як практично кожен з наведених способів може в певних випадках виступати складовою частиною будь-якого іншого з перерахованих або декілька методів можуть використовуватися в комплексі.

1.2 Аналіз існуючих видів і методів захисту комп'ютера від НСД

Згідно з законом України «Про захист інформації в інформаційно-телекомунікаційних системах», захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [2].

Захист інформації від НСД – захист, що спрямований на попередження отримання захищеної інформації зацікавленими суб'єктами з порушенням нормативних та правових документів чи актів або встановлених власниками інформації прав чи правил розмежування доступу до захищеної інформації [3].

Особливості захисту комп'ютера та ІС від НСД обумовлені специфікою їх використання. Як правило, комп'ютером користується обмежене число користувачів. Комп'ютери можуть працювати як в автономному режимі, так і в складі локальних мереж (сполученими з іншими комп'ютерами) і можуть бути підключені до віддаленого комп'ютера або локальної мережі. Для захисту від НСД використовуються такі методи: ідентифікація, автентифікація, управління доступом і технічні засоби. Також можуть бути використані засоби шифрування, системи виявлення вторгнень та політика безпеки.

1.2.1 Ідентифікація

Ідентифікація - процедура, в результаті виконання якої для суб'єкта ідентифікації виявляється його ідентифікатор (унікальне ім'я або мітка), що однозначно ідентифікує цього суб'єкта в інформаційній системі. Для виконання процедури ідентифікації в ІС суб'єкту попередньо повинен бути призначений відповідний ідентифікатор (тобто, проведена реєстрація суб'єкта в інформаційній системі).

Процедура ідентифікації безпосередньо пов'язана з автентифікацією: суб'єкт проходить процедуру автентифікації, і, якщо вона успішна, то ІС на основі факторів автентифікації визначає ідентифікатор суб'єкта. При цьому

достовірність ідентифікації повністю визначається рівнем достовірності виконаної процедури автентифікації.

1.2.2 Автентифікація

Автентифікація - процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора[4]. В інформаційній безпеці автентифікація є частиною процедури надання доступу для роботи в ІС, яка йде після ідентифікації і перед авторизацією. Як спосіб автентифікації в ІС використовується попередня ідентифікація, яка базується на ідентифікаторі (логіну) та паролі, які призначаються користувачеві ІС. Пароль – це конфіденційна інформація, знаючи яку користувач може володіти певними ресурсами в системі. Після введення логіну і паролю користувачем, комп'ютер порівнює ці значення із тими, що знаходяться в захищеній базі даних, і якщо ця процедура є успішною, він авторизовує користувача з допуском до роботи в ІС.

Види автентифікації:

- однофакторна автентифікація. Традиційну автентифікацію за допомогою пароля ще називають слабкою. Тому що є певні ресурси та методи для перехоплення або підбору паролю, і злом стає можливим в залежності від витраченого часу. Також дуже велике місце займає людський фактор: якщо пароль є стійким до злому методом підбору, то його складніше пам'ятати, і тому зростає шанс, що даний пароль буде надруковано або виписано. Завдяки цьому, зростає імовірність перехоплення чи крадіжки паролю і подальшого взлому ІС. Але паролі, які легко запам'ятати людині не є дуже стійкими до злому. Через це можна використовувати одноразові паролі, але їх перехоплення або викрадення також є можливим;

- багатфакторна автентифікація. Разом із слабкою, при такій необхідності, використовується сильна або багатфакторна автентифікація, що заснована на основі двох або більшої кількості факторів. В цьому випадку для автентифікації використовується не тільки інформація, яка відома

користувачеві, але і додаткові чинники. Наприклад, такими чинниками можуть виступати властивість, якою володіє даний суб'єкт, якась інформація або знання, яку він знає чи використання якогось предмету, що є у суб'єкта.

Способи автентифікації:

а) парольний, який здійснюється на основі володіння користувачем визначеної конфіденційної інформації;

б) біометричний, що заснований на унікальності певних антропометричних характеристик людини. В області інформаційних технологій поняття біометрії застосовується у технологіях ідентифікації особистості. Біометричний захист ефективніший ніж такі методи, як використання смарт-карт, паролів, чи PIN-кодів. Найчастіше використовуються:

- 1) параметри голосу;
- 2) візерунок райдужної оболочки ока і карта сітківки ока;
- 3) риси обличчя;
- 4) форма долоні;
- 5) відбитки пальців;
- 6) форма і спосіб особистого підпису;

в) за допомогою унікального предмета. Здійснюється при наявності додаткових предметів, таких як токен автентифікації чи смарт-карти або особливих атрибутів, як криптографічний сертифікат.

1.2.3 Управління доступом

Логічне управління доступом – це механізм для систем з великою кількістю користувачів, що допомагає забезпечувати цілісність та конфіденційність певних об'єктів, а також забороняє використовувати систему неавторизованим користувачам, таким чином, забезпечуючи доступність ІС. Логічне управління доступом реалізується програмними засобами, у відмінності від фізичного управління. Засоби управління доступом можуть контролювати дії, які процеси чи користувачі, тобто, суб'єкти можуть або не можуть виконувати у системі на певними ресурсами або інформацією, тобто,

об'єктами. Таким чином, є певні сукупність суб'єктів і набір об'єктів. Завданням логічного управління доступом є те, щоб для кожної пари «суб'єкт-об'єкт» визначити безліч певних операцій, які допускаються, а також слідкувати за виконанням цих правил [5].

Відносини «суб'єкти-об'єкти» можна розглядати у вигляді матриці доступу, де у стовпцях знаходяться об'єкти, а у рядках – суб'єкти, а на перетині стовпців і рядків записані додаткові умови, наприклад, час і місце дії, а також – дозволені види доступу. Об'єктами можуть бути файли, процеси чи пристрої. Якщо об'єкти - це файли і пристрої, то до них можуть застосовуватись права на читання, запис або використання, якщо це програмні файли, а також – іноді на додавання та видалення. Також окремим правом може бути передача повноважень доступу, тобто володіння, іншим суб'єктам. Дані права для користувачів задаються адміністратором системи.

Для того, щоб чітко провести розмежування між санкціонованим (легальним) доступом і НСД необхідно ввести політику безпеки. Політика безпеки може бути описана формальним або неформальним чином. Формальний опис політики безпеки проводиться в рамках моделі безпеки. Таким чином, модель безпеки можна визначити, як абстрактний опис поведінки цілого класу систем, без розгляду конкретних деталей їх реалізації.

Розрізняють три основних види моделей політики безпеки (моделі розподілу доступу): дискреційні, мандатні і рольові.

Дискреційне (вибіркове) розмежування доступу характеризується розмежуванням доступу між званими суб'єктами і об'єктами. Суб'єкт з певним правом доступу може передавати це право будь-якого іншого суб'єкта, якщо він є власником. Для кожної пари суб'єкт-об'єкт має бути задано явне і не двозначне перерахування допустимих типів доступу (читання, запис, редагування тощо), які є санкціонованими для даного суб'єкта (індивідуум або група індивідуумів).

До вибіркової моделі можна віднести такі моделі доступу:

- розмежування доступу за списками;

- використання матриці повноважень.

Дискреційний метод розмежування доступу має ряд недоліків:

- у разі розмежування доступу за списками права доступу дуже розосереджені;
- права доступу існують окремо від даних або об'єктів, тому користувач, який має право доступу до секретної інформації, може це право передати кому-завгодно, навіть того, хто цього права не має.

Щоб уникнути дані загрози, формують матрицю доступу, яка не матиме протиріч в контексті суб'єкт-об'єкт.

Мандатне управління доступом більш досконале, ніж дискреційне. Для реалізації даного принципу до кожного суб'єкту і об'єкту надається відповідна класифікаційна мітка, яка відображає місце даного суб'єкта або об'єкта у відповідній ієрархії. За допомогою міток суб'єктам і об'єктам повинні бути призначені класифікаційні рівні (уразливості, категорії секретності, категорії обмеження доступу і т.п.), які є комбінацією ієрархічних і не ієрархічних категорій. Дані мітки є основою мандатного принципу розмежування доступу. Мандатний принцип розмежування доступу базується на тому, що ресурси ІС діляться на відповідності: за рівнем секретності та за категорією.

Комп'ютерна система захисту повинна реалізовувати мандатний принцип доступу до всіх об'єктів при явному або прихованому доступі з боку будь-якого суб'єкта. Через складність даного методу розмежування доступу, він використовується як доповнення до дискреційного методу розподілу доступу.

Рольовий метод розмежування доступу, ідеєю якого є прив'язка розмежування доступу до ролей, які призначаються кожному користувачеві, включає в себе підходи дискреційного і мандатного розмежування доступу. Щоб визначити зрозумілі і чіткі правила розмежування доступу для користувача ІС, формуються ролі. Це дозволяє також зробити більш гнучкими правила розмежування доступу, що динамічно змінюються при функціонуванні ІС. Найчастіше, рольовий метод використовується в ІС, де є чітка кількість користувачів та де достатньо точно визначено їх повноваження і обов'язки на

посадах. Тому, дуже складним завданням для невеликої кількості адміністраторів систем безпеки є зробити рольовий розподіл між великою кількістю користувачів, а саме де більше сотні ролей та дуже велика кількість дозволів, і між ними треба зробити певні взаємозв'язки та управляти дозволами і суб'єктами.

Треба визнати, що методи управління доступом не є повним вирішенням проблем захисту ІС від НСД. Це пов'язано з тим, що локальні засоби розмежування доступу не можуть спрогнозувати такі дії порушника, як, наприклад, завантаження і запуск шкідливого ПЗ, який буде слідкувати та аналізувати за мережним трафіком в ІС. Також, це може бути запис на зовнішній носій або друкування конфіденційної інформації, до якої у користувача був доступ. Для попередження наведених дій рекомендується впроваджувати системи активного моніторингу робочих комп'ютерів.

Також, методи розмежування віддаленого доступу не завжди впроможі забезпечити надійний захист від мережних атак, особливо від тих, що можуть проводитися користувачами локальної мережі. Дані атаки можливі завдяки вразливостям програмно-апаратного оснащення ІС, як серверів, так і робочих машин. Легкі паролі, помилки роботи, налаштування певних ПЗ можуть бути прикладами вразливостей. Для того, щоб розпізнавати дані атаки рекомендується використовувати засоби виявлення атак.

1.2.4 Технічні методи

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації [2].

Технічні засоби в основному реалізовані у вигляді електронних, електричних та електротехнічних пристроїв. Вся сукупність даних технічних

засобів поділяється на апаратні та фізичні. Апаратні засоби реалізуються у вигляді техніки або пристроїв, які сполучаються зі схожою апаратурою за стандартним інтерфейсом. Наприклад, система розпізнавання та розмежування доступу до інформації в ІС за допомогою паролів, кодів та іншої інформації. Під фізичними засобами розуміють у вигляді автономних пристроїв і систем, наприклад, замки на входних дверях та решітки на вікнах у приміщеннях, де знаходиться цінна апаратура. Також до фізичних засобів відносяться джерела безперебійного живлення та електромеханічне устаткування охоронної сигналізації, що розрізняється на зовнішні системи охорони, ультразвукові системи, телевізійні, радіолокаційні, системи контролю розтину апаратури та інші.

Висновки до розділу 1:

- були розглянуті основні існуючі види НСД, такі як навмисні та ненавмисні, програмні та технічні, а також – тактичні та стратегічні, і основні методи – агентурні та технічні;
- були проаналізовані методи захисту від НСД на основі ідентифікації, автентифікації, управлінням доступом, а також розглянуті технічні методи;
- практично кожен з наведених способів може в певних випадках виступати складовою частиною будь-якого іншого з перерахованих або декілька методів можуть використовуватися в комплексі;
- для найефективнішого захисту ІС від НСД треба використовувати комплекси даних методів разом із сучасними підходами, включаючи засоби розпізнавання мережних атак і контролювання робочих станцій. Слід приділити увагу засобам, де більше використовується автоматизація та можуть впроваджуватись методи, що є близькими до роботи людини, такі як ШНМ.

2 МЕТОДИ ШНМ ДЛЯ ЗАХИСТУ ВІД НСД ТА АНАЛІЗ ЇХ НЕДОЛІКІВ

2.1 Методи ШНМ для захисту від НСД

2.1.1 Поняття і класифікація ШНМ

Штучна нейронна мережа (ШНМ) - це частина обчислювальної системи, призначена для імітації того, як людський мозок аналізує та обробляє інформацію. Вона є основою штучного інтелекту і вирішує проблеми, які виявляються неможливими або складними за людськими або статистичними стандартами. ШНМ мають можливість самонавчання, яка дозволяє їм отримувати кращі результати, коли стає доступним більше даних. Першим моделюванням протікаючих у мозку людини процесів, були нейромережі У. Маккалока і У. Піттса [6]. Після розробки алгоритмів навчання, отримані моделі стали використовуватися в прикладних задачах, таких як: прогнозування, розпізнавання образів, управління та ін.

ШНМ побудовані подібно до мозку людини, вузли нейронів взаємопов'язані як павутина. Мозок людини має сотні мільярдів клітин-нейронів. Кожен нейрон складається з клітинного тіла, яке відповідає за обробку інформації, переносячи інформацію до (входів) і геть (виходів) від мозку [7].

ШНМ має сотні або тисячі штучних нейронів, їх називають процесорними одиницями, що взаємопов'язані вузлами. Схема штучного нейрона [6] представлена на рисунку 2.1. Ці одиниці обробки складаються з вхідних і вихідних одиниць. Блоки введення отримують різні форми та структури інформації на основі внутрішньої системи зважування, а нейронна мережа намагається дізнатись про представлену інформацію, щоб створити один вихідний звіт. Подібно до того, як люди потребують правил і вказівок для

отримання результату, ШНМ також використовують набір правил навчання, щоб вдосконалити свої результати.

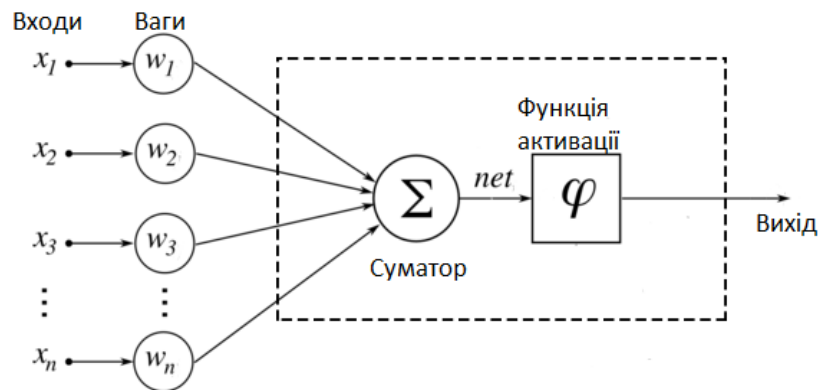


Рисунок 2.1 - Схема штучного нейрона

Спочатку ШНМ проходить фазу навчання, де вчиться розпізнавати закономірності в даних, візуально, на слух чи у тексті. Протягом цієї контрольованої фази мережа порівнює фактичний результат з тим, що передбачалося - бажаним результатом. Різниця між обома результатами коригується за допомогою зворотного розмноження. Це означає, що мережа працює в зворотному напрямку, переходячи від вихідного блоку до вхідних блоків, щоб відрегулювати вагу своїх з'єднань між блоками, поки різниця між фактичним та бажаним результатом не призведе до мінімально можливої помилки.

Існує величезна різноманітність різних архітектур, основні з яких будуть розглянуті нижче.

Класифікація ШНМ [6]:

а) класифікація за типом вхідної інформації:

- 1) аналогові нейронні мережі, що працюють з інформацією у виді дійсних чисел;
- 2) двійкові нейронні мережі, які використовують двійковий вигляд інформації;

3) прообразні нейронні мережі, що працюють з образною інформацією, тобто у вигляді знаків, ієрогліфів, символів;

б) класифікація за характером навчання:

1) навчання з учителем. Коли вихідний результат нейронної мережі відомо завчасно;

2) навчання без учителя. При такому навчанні нейромережа формує вихідний простір рішень тільки на основі вхідних даних. Також ці мережі називаються самоорганізаційними;

3) навчання з підкріпленням, коли є система, яка штрафує і заохочує вихідні результати в залежності від середовища;

в) класифікація за характером налаштування синапсів:

1) мережі з фіксованими зв'язками, коли коефіцієнти ваг нейронної мережі вибираються виходячи з умов задачі одразу;

2) мережі з динамічними зв'язками, де налаштування синаптичних зв'язків виконується у процесі навчання мережі;

г) класифікація за характером зв'язків:

1) мережі прямого поширення. У таких мережах всі зв'язки йдуть чітко від вхідних до вихідних нейронів. Як прикладами можуть бути такі мережі: перцептрон Розенблатта чи багат шаровий перцептрон або мережі Ворда;

2) рекурентні нейронні мережі. Результат з виходу або з прихованого шару нейронів частково передається назад до входів нейронів вхідного шару, це називається зворотним зв'язком. Одним із варіантів рекурентних мереж є двонаправлені мережі, у яких існують зв'язки у двох напрямках: як від вхідного до вихідного, так і навпаки між шарами нейронів;

3) радіально-базисні функції. ШНМ, що використовують радіально-базисні функції задля активації.

Окремо будуть розглянуті згорткові нейронні мережі (ЗНМ). Цей вид мережі дуже відрізняється від інших, так як в основному використовується для роботи з графічною і аудіо інформацією. Модель такої мережі [8] представлена

на рисунку 2.2. Ця архітектура обробляє дані не цілком, а фрагментами, але при цьому дані не дробляться на частини, а здійснюється свого роду послідовний прогін. Потім дані передаються далі по верствам. Крім згорткових шарів (С) використовуються також шари об'єднання (Р - pooling). Наприклад, з аудіодоріжки вибираються тільки ключові моменти: піки амплітуд і паузи. Шари об'єднання стискаються з глибиною (зазвичай ступенем двійки). До кінцевих верств додаються кілька персептронів (мережа прямого поширення), для подальшої обробки даних.

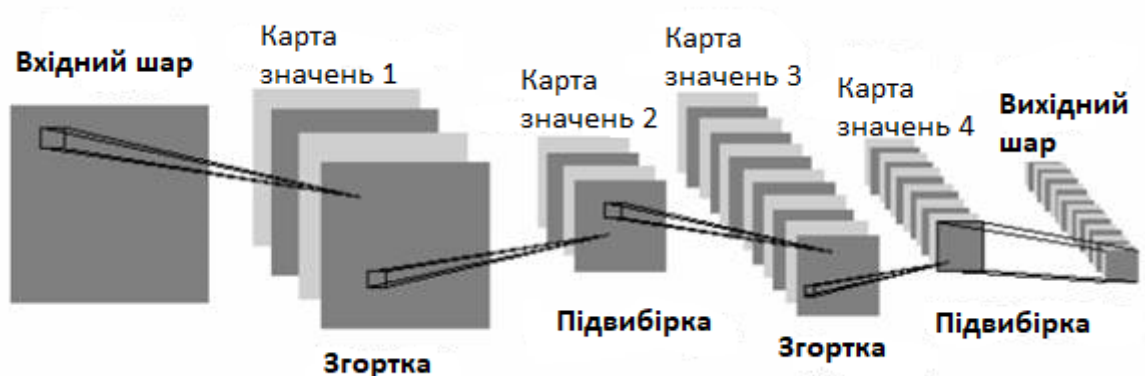


Рисунок 2.2 - Модель ЗНМ

Ця архітектура є найбільш придатною для розпізнавання зображень і їх класифікації. Також, ЗНМ використовуються у відеоаналізі, обробці природної мови, також можуть бути використані для аналізу документів та текстів. З її допомогою можливо розпаралелювання обчислень, і, як наслідок, використання графічних процесорів. Однак, ця архітектура потребує налаштування великої кількості варійованих параметрів, таких як кількість шарів, кількість ядер в кожному шарі, функції активації кожного нейрона і багато інших.

Капсульні нейронні мережі (КНМ) являють собою систему машинного навчання, яка є одним з видів штучної нейронної мережі, які можуть бути використані для моделі ієрархічних відносин. Підхід - це спроба більш тісно імітувати біологічну нейронну організацію.

Ідея полягає в тому, щоб додати структури, що називаються «капсулами», до ЗНМ і повторно використовувати вихід з декількох цих капсул, щоб сформувати більш стабільні виходи для вищих капсул. Вихід - це вектор, що складається з ймовірності спостереження та пози для цього спостереження. Цей вектор схожий на те, що робиться, наприклад, при класифікації з локалізацією в ЗНМ.

Застосування ШНМ [6]:

- прийняття рішень і управління;
- кластеризація, тобто роздроблення множини вхідних сигналів на класи, враховуючи те, що заздалегідь не відомі кількість та ознаки класів. Це можуть виконувати, наприклад, нейромережі Кохонена;
- прогнозування. ШНМ здатні виділяти та узагальнювати приховані залежності між даними на вході та виході, тому і здатні прогнозувати;
- апроксимація. ШНМ мають здатність апроксимувати безперервні функції;
- стиснення даних і асоціативна пам'ять;
- аналіз даних;
- оптимізація;
- розпізнавання образів і класифікація. У якості образів можуть бути різні за походженням об'єкти, такі як тестові символи, зображення, звуки і т.п. Для навчання мережі потрібні різні зразки образів із поясненням їх класовості, тобто, до якого саме класу дані зразки належать. Зазвичай, зразок представляється у векторному вигляді зі значенням ознак, і якщо їх недостатньо мережа може некоректно співвіднести один і той самий зразок з кількома класами. Якщо мережа навчилася коректно, то вона буде співвідносити невідомі їй образи до певних класів. Зазвичай, топологія такої мережі визначається тим, що кількість визначених класів, як правило, дорівнює кількості нейронів у вихідному шарі. І також між виходом ШНМ і класом, що йому співвідноситься встановлюється відповідність. Коли мережі дається на

розпізнавання образ, то повинна з'явитись ознака приналежності образу до певного класу на одному з її виходів. А на інших виходах повинна бути ознака неналежності образу до класу, і якщо на кількох виходах є приналежність до класу, то така мережа вважається не впевненою у своєму виборі.

2.1.2 Застосування ШНМ в захисті від НСД

Основні завдання, які можуть вирішуватися методами ШНМ в сфері забезпечення інформаційної безпеки і захисту від несанкціонованого доступу:

- швидке розпізнавання кіберзагроз;
- оптимізація процесу пошуку шкідливих джерел;
- прийняття до уваги тих відомостей про систему, які можуть здатися несуттєвими неінтелектуальній системі захисту, тим самим знижуючи ризик;
- боротьба зі шкідливим ПЗ;
- внесення певних відомостей в процесі навчання і побудова на їх основі більш потужної системи захисту;
- обслуговування засобів управління ідентифікацією, автентифікацією і доступом до ресурсів, а також засобів адміністрування доступу;
- усучаснення антивірусного програмного забезпечення;
- використання в засобах виявлення атак;
- використання в брандмауерах;
- використання в криптографії.

2.2. Аналіз недоліків ЗНМ

Згорткові нейронні мережі є надзвичайно гнучкими моделями машинного навчання, які спочатку були засновані на принципах, як теоретично працює мозок. Основними будівельними блоками нейронної мережі є

«згорткові» шари. Вони беруть необроблену інформацію зі старого рівня, знаходять в ній шаблони і відправляють її на наступний рівень, щоб надати сенс ширшій картині.

Проблема ЗНМ полягає в тому, що у них занадто мало рівнів підструктур, і що потрібно згрупувати нейрони в кожному шарі в «капсули», такі як міні-стовпці, які роблять багато внутрішніх обчислень, і тоді вивести підсумковий результат [10].

Основні недоліки ЗНМ [10]:

- об'єднання втрачає інформацію. ЗНМ використовує «об'єднання» або еквівалентні методи, щоб «підсумовувати» те, що відбувається в менших областях і обробляти все більші шматки зображення. Це рішення, яке змусило ЗНМ працювати ефективно, але воно втрачає цінну інформацію. Капсульні мережі будуть обчислювати позу, взаємозв'язок між більш дрібними об'єктами, щоб скласти більш великий об'єкт. Ця втрата інформації призводить до втрати просторової інформації;

- ЗНМ не враховують просторові відносини між частинами зображення. Тому вони також занадто чутливі до орієнтації. При виборі і об'єднання і втрачаються точні просторові відносини між частинами більш високого рівня. Точні просторові відносини необхідні для розпізнавання. ЗНМ не враховують просторові відносини між базовими об'єктами. Маючи ці плоскі шари нейронів, які світяться в залежності від того, які об'єкти вони бачили, вони розпізнають наявність таких об'єктів. Але потім вони передаються на інші рівні активації та об'єднання і на наступний рівень нейронів (фільтрів), що не розпізнають, якими є взаємозв'язки між цими об'єктами в цьому єдиному шарі. Капсульні мережі, навпаки, представляють спрямованість поряд з контентом і з'єднуються між капсулами нейронів, щоб вивести просторові відносини і зберегти інформацію про пози. Відсутність згрупованого уявлення капсули, розрахунок пози і перевірка перекриття між капсулами призводить до наступної проблеми;

– ЗНМ не можуть перенести розуміння геометричних відношень на нові точки зору. Це робить їх більш чутливими до самого вихідного зображення, щоб класифікувати його в одну і ту ж категорію [8]. ЗНМ відмінно підходять для вирішення проблем з даними, аналогічними тим, на яких вони були навчені. Вони можуть класифікувати зображення або об'єкти всередині них, що дуже близько до речей, які вони розпізнали раніше. Але якщо об'єкт повернути, зробити під іншим кутом, особливо в 3D, нахилити або зробити іншу орієнтацію, ніж та, на якій навчалась ЗНМ - мережа не розпізнає це ефективно і правильно. Одним з рішень є штучно створити похиле зображення або групи зображень і додати їх в набір для навчання, однак цього все ще не вистачає принципово більш надійної структури.

Висновки до розділу 2:

- у даному розділі були описані поняття ШНМ і їх класифікація;
- ШНМ впроваджується у різні аспекти життя людини та в автоматизацію комп'ютерних і інформаційних систем, тому їх важливо використовувати і для захисту від НСД;
- були розглянуті ЗНМ, які найефективніше використовуються у задачах розпізнавання і класифікації як зображень, так і відео, тексту та мови, що робить даний вид мереж достатньо широко використовуваним у задачах забезпечення безпеки ІС від НСД;
- ЗНМ мають ряд недоліків, таких як: втрата інформації, ігнорування просторових відносин і не чутливість до зміни положення. Дані недоліки вирішуються новим капсульним методом ШНМ, який буде проаналізовано у наступному розділі.

3 АНАЛІЗ КАПСУЛЬНОГО МЕТОДУ

3.1 Капсульний метод

У класичних ЗНМ кожен нейрон в першому шарі представляє піксель. Потім він передає цю інформацію в наступні шари. Наступні згорткові шари групують групу нейронів разом, так що один нейрон там може являти собою цілий каркас (групу) нейронів. Таким чином, він може навчитися представляти групу пікселів, особливо, якщо є багато таких прикладів в наборі даних, і нейронна мережа навчиться збільшувати вагу цього нейрона.

Однак цей метод концентрується виключно на існуванні об'єкта на зображенні навколо певного місця, але він нечутливий до просторових відносин і напрямку об'єкта. Даний метод найчастіше використовується у задачах розпізнавання людського обличчя на графічному зображенні, тому і особливості його роботи будуть описані таким чином.

3.1.1 Концепція капсульного методу

Капсульний метод - це нова концепція, яка може містити більше інформації про кожен «об'єкт». Капсули - це вектор (елемент з розміром і напрямком), що вказує функції об'єкта і його ймовірність [9]. Ці функції можуть бути будь-якими з параметрів створення екземплярів, таких як «поза» (положення, розмір, орієнтація), деформація, швидкість, відображення світла, відтінок, текстура і т.д.

Так, наприклад, нейронна мережа може навчитися мати одну капсулу, що представляє «очі», яка буде містити інформацію про всі варіаціях очей, які вона бачила, а не різні нейрони для різних варіацій очей. Наприклад, крім інформації про групу пікселів, що виглядає «оком», капсула також може вказувати свої атрибути, такі як кут і розмір, щоб вона могла представляти з

однаковою загальною інформацією про різні очі, якщо буде змінюватися цей кут або розмірні параметри.

Капсульна нейронна мережа буде розпізнавати підструктури, присутні у великій картині, разом з інформацією про розташування і напрямку цих елементів.

Тепер, як у нейронної мережі є шари нейронів, так і у капсульної мережі можуть бути шари капсул. Таким чином, можуть бути вищі капсули, що представляють групу об'єктів (капсул) під ними. Капсула є більш гнучкою і надійною у виявленні цих особливостей в цілому ряді варіацій[9].

Ця інтелектуальна капсула може використовувати цю інформацію для кращої ідентифікації. Якщо всі ці функції однаково повернені і виміряні, це означає, що ця мережа може ідентифікувати об'єкти, навіть якщо вони перетворені з вихідного введення. Якщо ні, то це зображення з меншою ймовірністю [9].

КНМ може краще класифікувати на основі невідповідностей в орієнтації і розмірі для ідентифікації. Якщо субелементи, наприклад, ніс, очі і рот несумісні за своєю орієнтацією і розміром один з одним, тоді вищі капсули помітять і будуть менш упевнені в результаті. Це не можна зробити з нормальними нейронами в ЗНМ: там була тільки ймовірність того, що група пікселів буде виглядати якось без інформації про її напрямки. Порівнюючи сумісність кожної особливості капсули можна виявити, що вони несумісні.

3.1.2 Точка зору інваріантності та стійкість до змагальної атаки

Класична ЗНМ може розпізнавати тільки особу, ґрунтуючись на аналогічному детекторі особи, що зберігається з аналогічною орієнтацією і розміром. Це тому, що риси обличчя зберігаються в місцях усередині рамки пікселів. Тоді він буде розпізнавати тільки зображення, які мають схожі риси в схожих місцях на зображенні. Отже, він повинен мати окремі уявлення для різних варіацій обличчя. Ці уявлення в кінцевому підсумку будуть

співставленні з одним і тим же класом, але це все ще означає, що ЗНМ повинна попередньо побачити досить великий масив прикладів кожного типу перетворення, щоб створити його внутрішнє подання і розпізнати його в майбутньому. Навпаки, капсульна мережа може мати загальне уявлення і перевіряти, яка трансформація (обертання, розмір і т.д.), а також, чи всі функції повернені або перетворені в тій же кількості і напрямку. Нейронна мережа може безпосередньо виявити, що цей набір підструктур дійсно еквівалентний більш високій структурі, перетвореної на ту ж величину. Це означає, що КНМ узагальнює клас замість того, щоб запам'ятовувати кожен варіант точки зору класу, тому він інваріантний до точки зору.

Оскільки метод є інваріантом точки зору, це означає, що:

- це більш стійко до змін в орієнтації і розмірі введення;
- це потребує набагато менше даних, які часто важко отримати, а також внутрішні уявлення. Таким чином, можна більш ефективно правильно класифікувати.

Це означає, що КНМ може визначити нові, невидимі варіації класу без навчання. Концептуально, це більше схоже на те, як розпізнає образи людина. Наприклад, замість того, щоб запам'ятати обличчя, коли ніс знаходиться на висоті 1,70 м, а рот - на 1,67 м, людина зберігає відносини між ротом і носом і, таким чином, може виявити їх в будь-якому варіанті[9]. Це називається еквіваріантність капсул, тобто виявлення класу об'єктів, які можуть перетворювати один до одного (тобто обертанням, зміщенням або будь-яким іншим перетворенням). Крім розпізнавання тільки самого об'єкта і його перетворення, вони також виявляють, в якому стані трансформації знаходиться об'єкт саме зараз. Модель вивчає варіанти функцій в одній капсулі, щоб більш ефективно екстраполювати можливі варіанти з меншою кількістю навчальних даних.

Тому, коли об'єкт переміщується, нахиляється або має інший розмір, це той же базовий об'єкт, капсула все ще виявить цей об'єкт з високою ймовірністю. Це можливо, тому що капсула містить інформацію про об'єкт в

векторі, довжина якого дорівнює ймовірності, тому довжина не зміниться, якщо об'єкт перетвориться, а його напрямок до розмірів перетворення, яке він представляє, зміниться.

Таке більш надійне уявлення об'єктів може зробити його більш стійким до змагальних атак. Змагальні атаки - це метод, щоб «обдурити» нейронну мережу, щоб визначити, що об'єкт - це насправді щось інше, шляхом підстроювання пікселів на зображенні майже непомітним для людського ока, але тільки в тих напрямках, які представляють нейронні мережі іншим об'єктом, поки мережа не вирішить, що це інший об'єкт. Наявність більш узагальненого, корисного і надійного уявлення цього об'єкта, зокрема, з точки зору незмінності точок зору і стійкості до змін об'єкта, може допомогти мережі постійно розпізнавати, що це один і той самий об'єкт, і, таким чином, пом'якшує ці атаки.

Це важливо для випадків, коли розпізнавання нейронних мереж визначає реальні події: наприклад, виявлення самотійного водіння автомобіля під стоп-знаки. Добре освічений злочинець може наклеїти на цей знак майже невидиму наклейку і «зламати» машину, щоб розпізнати цей знак як «Допустима швидкість- 60 км» і продовжувати рух. Але система, заснована на КНМ, а не на ЗНМ, була б набагато більш стійкою до таких ворожих атак.

3.2 Структура та обчислювальні етапи капсули

3.2.1 Порівняння капсули зі штучними нейронами

У таблиці 3.1 наведені порівняння капсули і штучного нейрону. Згідно наведеної таблиці, слід зазначити, що нейрон отримує вхідні скаляри від інших нейронів, а потім помножує їх на скалярні ваги та суми. В подальшому ця сума передається одній із безлічі можливих функцій нелінійної активації, яка приймає вхідний скаляр і виводить скаляр відповідно до функції. Цей скаляр буде результатом нейрона, який буде подано як вхід до інших нейронів.

Таблиця 3.1 - Важливі відмінності між капсулами та нейронами.

Вхід з нижчого рівня капсули/нейрону		Вектор (u_i)	Скаляр (x_i)
Операції	Афінне перетворення	$\hat{u}_{j i} = W_{ij}u_i$	--
	Зважування	$s_j = \sum_i c_{ij} \hat{u}_{j i}$	$a_j = \sum_i w_i x_i + b$
	Сума		
	Нелінійна активація	$v_j = \frac{\ s_j\ ^2}{1 + \ s_j\ ^2} \frac{s_j}{\ s_j\ }$	$h_j = f(a_j)$
Вихід		Вектор (v_j)	Скаляр (h_j)

Таким чином, штучний нейрон можна описати трьома етапами:

- скалярне зважування вхідних скалярів;
- сума зважених вхідних скалярів;
- скалярно-скалярна нелінійність.

З іншого боку, капсула має векторні форми вищевказаних 3-кроків на додаток до нового кроку, афінним перетворенням введення:

- матричне множення вхідних векторів;
- скалярне зважування вхідних векторів;
- сума зважених вхідних векторів;
- нелінійність вектор-вектор.

3.2.2 Обчислювальні етапи капсули

Розглянемо обчислювальні етапи, що відбуваються всередині капсули:

- матричне множення вхідних векторів. Вхідні вектори, які отримує капсула, надходять із 3 інших капсул у шарі нижче. Довжини цих векторів кодують ймовірності того, що капсули нижнього рівня виявляють їх відповідні об'єкти, а напрямки векторів кодують деякий внутрішній стан виявлених

об'єктів. Припустимо, що капсули нижнього рівня виявляють очі, рот і ніс відповідно, а зовнішня капсула виявляє обличчя. Ці вектори потім множать на відповідні вагові матриці, які кодують важливі просторові та інші взаємозв'язки між рисами нижчого рівня (очі, рот і ніс) та особливостями вищого рівня (обличчя). Наприклад, матриця може кодувати взаємозв'язок між носом і обличчям: обличчя зосереджено навколо носа, його розмір в 10 разів перевищує розмір носа, а його орієнтація в просторі відповідає орієнтації носа, оскільки всі вони лежать в одній площині. Після множення на ці матриці отримується передбачуване положення функції вищого рівня. Це повинно мати такий вигляд: якщо ці 3 передбачення характеристик нижчого рівня вказують на одне положення і стан обличчя, то це повинно бути обличчя, як схематично зображено на рисунку 3.1;



Рисунок 3.1 - Прогнози щодо місця розташування капсул носа, рота та очей близько збігаються: там повинно бути обличчя

– скалярне зважування вхідних векторів. Штучний нейрон зважує свої входи до їх додавання. У випадку з нейроном, ці ваги використовуються під час зворотного розповсюдження, але у випадку з капсулою, - вони визначаються за допомогою «динамічної маршрутизації», що є новим способом визначити, куди йде вихід кожної капсули. Є одна капсула нижнього рівня, якій потрібно "визначитися", до якої капсули вищого рівня вона відправить свій вихід. Він прийме своє рішення, регулюючи ваги, які помножить вихід цієї капсули, перш ніж надсилати її вліво чи вправо капсули вищого рівня. Тепер капсули вищого рівня вже отримали багато вхідних векторів від інших капсул нижчого рівня. Якщо ці точки згуртовуються, це означає, що прогнози капсул нижчого рівня близькі один до одного. Отже, куди капсула нижнього рівня повинна надсилати свій вихід, пояснює алгоритм динамічної маршрутизації. Вихід нижньої капсули при множенні на відповідну матрицю, розташовується далеко від червоного скупчення «правильних» прогнозів у капсулі. З іншого боку, він приземлиться дуже близько до "справжніх" прогнозів у правій капсулі. Капсула нижнього рівня має механізм вимірювання того, яка капсула верхнього рівня краще відповідає її результатам і автоматично регулює її вагу таким чином, щоб вага відповідна правій капсулі буде велика, а вага, відповідна лівій капсулі, буде низькою;

– сума зважених вхідних векторів. Цей крок схожий на звичайний штучний нейрон і являє собою комбінацію входів;

– "Сквош": нова нелінійність між вектором. Ще одне нововведення, яке впроваджує КНМ, - це нова нелінійна функція активації, яка приймає вектор, а потім масштабує її довжину не більше 1, але не змінює свого напрямку. Імовірність того, що зображення буде класифікувати як j обчислюється за величиною v_j у формулі 3.1 [11].

$$v_j = \frac{\|s_j\|^2}{1 + \|s_j\|^2} \frac{s_j}{\|s_j\|}, \quad (3.1)$$

де $\frac{\|s_j\|^2}{1+\|s_j\|^2}$ – додаткове масштабування (сквош);

$\frac{s_j}{\|s_j\|}$ – масштабування вхідного вектору.

Розсіювання нелінійності масштабує вхідний вектор без зміни напрямку.

У формулі 3.1 права частина рівняння масштабує вхідний вектор так, щоб він мав одиничну довжину, а ліва здійснювала додаткове масштабування. Довжина вектору виходу може бути інтерпретована як ймовірність виявлення певної ознаки капсулою.

3.3 Динамічна маршрутизація між капсулами

Динамічна маршрутизація між капсулами - новий алгоритм динамічної маршрутизації, який дозволяє тренувати капсульні мережі [11]. Схематично зображена на рисунку 3.2, та алгоритм наведено у таблиці 3.2.

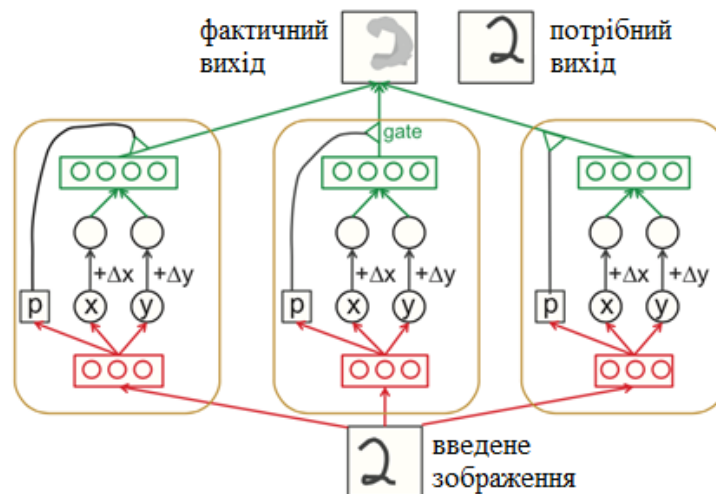


Рисунок 3.2 – Схематичне зображення капсул та маршрутів між ними[15]

Таблиця 3.2– Алгоритм динамічної маршрутизації [11]

Procedure 1 Routing algorithm.	
1: procedure ROUTING($\hat{\mathbf{u}}_{j i}, r, l$)	
2: for all capsule i in layer l and capsule j in layer $(l + 1)$: $b_{ij} \leftarrow 0$.	
3: for r iterations do	
4: for all capsule i in layer l : $\mathbf{c}_i \leftarrow \text{softmax}(\mathbf{b}_i)$	▷ softmax computes Eq. 3
5: for all capsule j in layer $(l + 1)$: $\mathbf{s}_j \leftarrow \sum_i c_{ij} \hat{\mathbf{u}}_{j i}$	
6: for all capsule j in layer $(l + 1)$: $\mathbf{v}_j \leftarrow \text{squash}(\mathbf{s}_j)$	▷ squash computes Eq. 1
7: for all capsule i in layer l and capsule j in layer $(l + 1)$: $b_{ij} \leftarrow b_{ij} + \hat{\mathbf{u}}_{j i} \cdot \mathbf{v}_j$	
return $\mathbf{v}_j$	

Розглянемо таблицю 3.2: перший рядок говорить про те, що ця процедура приймає всі капсули на нижчому рівні l та їх результати $\hat{\mathbf{u}}$, а також кількість ітерацій маршрутизації r . Останній рядок показує те, що алгоритм буде виводити випуск капсули більш високого рівня $\mathbf{v}_j$. По суті, цей алгоритм демонструє, як обчислити передачу вперед мережі. У другому рядку можна помітити, що є новий коефіцієнт b_{ij} , який є просто тимчасовим значенням, що буде ітераційно оновлено, і після закінчення процедури його значення буде збережено в c_{ij} . На початку тренінгу значення b_{ij} ініціалізується на нулі. У рядку 3 сказано, що кроки в 4–7 будуть повторені r разів (кількість ітерацій маршрутизації). Крок i у рядку 4 обчислює значення вектора $\mathbf{c}_i$, яке є всіма маршрутними вагами для капсули нижнього рівня i . Це робиться для всіх капсул нижнього рівня. Softmax переконається, що кожна вага c_{ij} є негативним числом, і їх сума дорівнює одиниці. По суті, softmax виконує імовірнісний характер коефіцієнтів c_{ij} .

При першій ітерації значення всіх коефіцієнтів c_{ij} буде рівним, бо по лінії два всі b_{ij} встановлюються на нуль. Наприклад, якщо у нас є 3 капсули нижнього рівня та 2 капсули вищого рівня, то c_{ij} дорівнює 0,5. Статична всіх c_{ij} рівність при ініціалізації алгоритму представляє стан максимальної плутанини та невизначеності: капсули нижчого рівня не мають уявлення, які капсули вищого рівня найкраще відповідають їх виходу. Звичайно, що процес повторюється, і ці рівномірні розподіли будуть змінюватися.

Адже ваги c_{ij} були розраховані для всіх нижчих рівнів капсул, можна перейти до рядку 5, де будуть розглянуті капсули вищого рівня. Цей крок обчислює лінійну комбінацію вхідних векторів, зважених коефіцієнтами маршрутизації c_{ij} , визначені на попередньому кроці. Інтуїтивно це означає зменшення вхідних векторів та їх додавання разом, що створює вихідний вектор c_{ij} . Це робиться для всіх капсул вищого рівня. Далі, у рядку 6, вектори з останнього кроку проходять через нелінійність сквошу, що гарантує збереження напрямку вектора, але його довжина примушує бути не більше 1. Цей крок створює вихідний вектор v_j для всіх капсул вищого рівня.

Кроки 4–6 просто обчислюють вихід капсул вищого рівня. Крок по лінії 7 - це місце, де відбувається оновлення вагів. Цей крок відображає суть алгоритму маршрутизації. Цей крок розглядає кожну капсулу вищого рівня j , а потім вивчає кожен вхід і оновлює відповідну вагу b_{ij} за формулою. Формула говорить, що нове значення ваги дорівнює старому значенню плюс крапковий добуток поточного виходу капсули j і вхід в цю капсулу з капсули нижнього рівня i . Точковий виріб розглядає подібність між входом у капсулу та виходом із капсули. Крім того, капсула нижнього рівня направить свій вихід на капсулу вищого рівня, вихід якої аналогічний. Ця схожість фіксується точковим твором. Після цього кроку алгоритм починається з кроку 3 і повторює процес r разів.

Після r разів були розраховані всі виходи для капсул вищого рівня та встановлено вагу маршрутизації. Передача вперед може продовжуватися до наступного рівня мережі.

3.4 Архітектура КНМ

КНМ має 2 частини: кодер і декодер. Перші 3 шари є кодером, а інші 3 – декодером [12]:

- шар 1. Згортковий шар;

- шар 2. Шар первинних капсул;
- шар 3. Шар DigitCaps;
- шар 4. Повністю з'єднаний №1;
- шар 5. Повністю з'єднаний №2;
- шар 6. Повністю з'єднаний №3.

3.4.1 Кодер

Архітектура кодера КНМ зображена на рисунку 3.3.

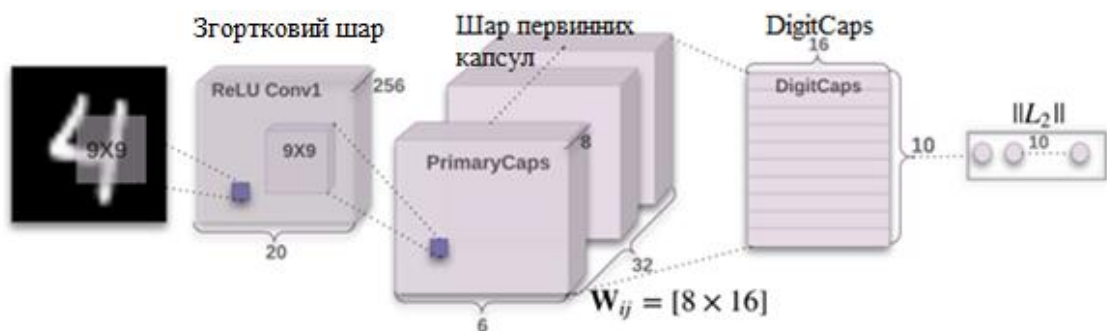


Рисунок 3.3 - Архітектура кодера КНМ [11]

Частина мережі кодування приймає за вхід зображення MNIST (база даних зразків рукописного написання цифр) 28x28 і вчиться кодувати її в 16-мірний вектор параметрів інстанції, саме тут капсули виконують свою роботу. Вихід мережі під час прогнозування - це 10-мірні вектори довжини виходів. Декодер має 3 шари: два з них згорнуті, а останній повністю пов'язаний [13].

Шар 1. Згортковий шар:

- вхід: зображення 28x28 (один кольоровий канал);
- вихід: тензор 20x20x256;
- кількість параметрів: 20992.

Завдання згорткового шару - виявити основні особливості в 2D зображенні. У КНМ згортковий шар містить 256 ядер розміром 9x9x1 та кроком

1, з подальшою активацією випрямовувачем. Щоб обчислити кількість параметрів, також потрібно врахувати, що кожне ядро в згортковому шарі має 1 зміщення. Отже, цей шар має $(9 \times 9 + 1) \times 256 = 20992$ відслідковуваних параметри загалом.

Шар 2. Шар первинних капсул:

- вхід: тензор $20 \times 20 \times 256$;
- вихід: тензор $6 \times 6 \times 8 \times 32$;
- кількість параметрів: 5308672.

Цей шар має 32 первинні капсули, завдання яких - брати основні ознаки, виявлені згортковим шаром, та створити поєднання ознак. У шарі є 32 «первинні капсули», які за своєю природою дуже схожі на згортковий шар. Кожна капсула застосовує вісім ядер $9 \times 9 \times 256$ (з кроком 2) до вхідного об'єму $20 \times 20 \times 256$ і, таким чином, виробляє вихідний тензор $6 \times 6 \times 8$. Оскільки є 32 такі капсули, об'єм виходу має форму $6 \times 6 \times 8 \times 32$. Зробивши обчислення, аналогічне попередньому шару, отримуємо 5308672 відслідковуваних параметрів у цьому шарі.

Шар 3. Шар DigitCaps:

- вхід: тензор $6 \times 6 \times 8 \times 32$;
- вихід: матриця 16×10 ;
- кількість параметрів: 1497600.

Цей шар має 10-значні капсули, по одній на кожну цифру. Кожна капсула бере в якості тензора $6 \times 6 \times 8 \times 32$. Можна вважати це 8-мірними векторами $6 \times 6 \times 32$, що становить 1152 вхідних вектора. Відповідно до внутрішніх функцій капсули, кожен з цих вхідних векторів отримує власну вагову матрицю 8×16 , яка відображає 8-мірний вхідний простір на 16-мірний вихідний простір капсули. Так, для кожної капсули існує 1152 матриць, а також коефіцієнти 1152 s та коефіцієнти 1152 b , що використовуються в динамічній маршрутизації. Помноживши: $1152 \times 8 \times 16 + 1152 + 1152$, ми отримуємо

149760 відслідковуваних параметрів на капсулу, потім множимо на 10, щоб отримати остаточну кількість параметрів для цього шару.

Функція втрати дуже схожа на функцію втрати методу опорного вектору. Вихід шару DigitCaps становить 10 шістнадцятивимірних векторів. Під час тренінгу, для кожного прикладу тренінгу, буде розраховано одне значення втрат для кожного з 10 векторів за формулою нижче, а потім 10 значень будуть додані разом для обчислення кінцевих втрат. Оскільки йдеться мова про контрольоване навчання, кожен навчальний приклад матиме правильну мітку, і у цьому випадку це буде десятивимірний одноколіїний вектор з 9 нулями та 1 у правильному положенні. У формулі 3.2 функції втрати правильна мітка визначає значення T_c : це 1, якщо правильна мітка відповідає цифрі цього конкретного DigitCap, а 0 - інакше. Рівняння функції втрати [9] наведено у формулі 3.2.

$$L_c = T_c \max(0, m^+ - \|v_c\|)^2 + \lambda(1 - T_c) \max(0, \|v_c\| - m^-)^2, \quad (3.2)$$

де L_c – термін втрати для одного DigitCap;

T_c – правильна мітка DigitCap;

$\max(0, m^+ - \|v_c\|)^2$ – нульові втрати при правильному прогнозуванні з імовірністю більше 0,9, і ненульовий в іншому випадку;

λ – константа, що використовується для числової стабільності;

$(1 - T_c)$ – 1, коли коректний DigitCap, а 0 – якщо некоректний;

$\max(0, \|v_c\| - m^-)^2$ – нульові втрати при некоректному прогнозуванні з імовірністю менше 0,1, і ненульові – в іншому випадку.

Згідно формули 3.2, припустимо, що правильна мітка дорівнює 1, це означає, що перший DigitCap відповідає за кодування присутності цифри 1. Для цієї функції втрати DigitCap T_c буде один, і на всі інші дев'ять DigitCaps T_c буде 0. Коли T_c дорівнює 1, тоді обчислюється перший член функції втрати, а другий

стає нульовим. Для цього прикладу, щоб обчислити втрату першого DigitCap, треба взяти вихідний вектор цього DigitCap і відіняти його від m^+ , який фіксується на рівні 0,9. Тоді зберігаємо отримане значення лише в тому випадку, коли воно більше нуля, і квадратне його. В іншому випадку повернеться 0. Іншими словами, втрата буде нульовою, якщо правильний DigitCap прогнозує правильну мітку з більшою ймовірністю 0,9, і буде ненульовою, якщо ймовірність менша 0,9.



Рисунок 3.4 - Значення функції втрати для правильного та неправильного DigitCap [14]

Згідно з рисунку 3.4, червоний графік "розрізаний" вертикально порівняно із зеленим. Це пояснюється лямбда-множником з формули.

Для DigitCaps, які не відповідають правильній етикетці, T_c буде нульовим, тому другий доданок буде оцінено (відповідає $(1 - T_c)$ частина). У цьому випадку можна побачити, що втрата буде нульовою, якщо невідповідний DigitCap прогнозує неправильну мітку з ймовірністю менше 0,1 та ненульовою, якщо вона передбачає неправильну мітку з ймовірністю більше 0,1.

У формулу коефіцієнт лямбда включається для чисельної стійкості під час тренувань (його значення фіксується в 0,5). Два терміни у формулі мають квадрати, оскільки ця функція втрати має L_2 норму, і ця норма працює краще.

3.4.2 Декодер

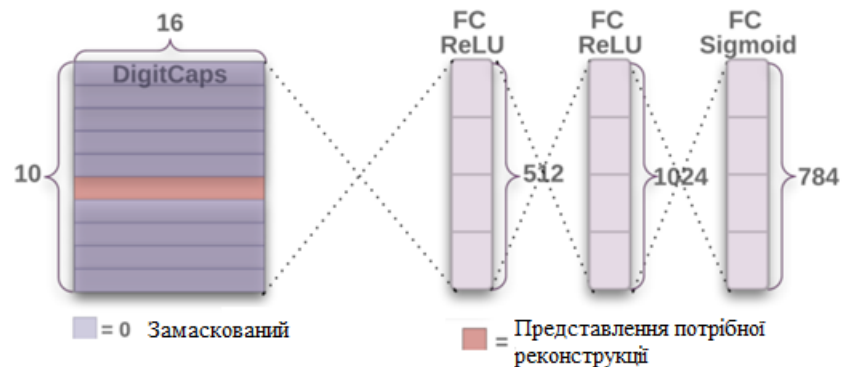


Рисунок 3.5 - Архітектура декодера КНМ [11]

Архітектура декодера зображена на рисунку 3.5. Декодер бере 16-мірний вектор з правильного DigitCap і вчиться його розшифровувати на зображення цифри, він використовує лише правильний вектор DigitCap під час тренування і ігнорує неправильні. Декодер використовується як регуляризатор, він приймає вихід правильного DigitCap як вхідний і вчиться відтворювати зображення розміром 28 на 28 пікселів, при цьому, функцією втрати є евклідова відстань між реконструйованим зображенням і вхідним зображенням. Декодер змушує капсули вивчити функції, корисні для реконструкції вихідного зображення. Чим ближче реконструйоване зображення до вхідного зображення, тим краще. Приклади реконструйованих зображень можна побачити на рисунку 3.6.



Рисунок 3.6 - Верхній ряд: оригінальні зображення. Нижній ряд: реконструйовані зображення [11]

Шар 4. Повністю з'єднаний №1:

- вхід: 16x10;
- вихід: 512;
- кількість параметрів: 82432.

Кожен вихід нижнього рівня отримує зважування і спрямовується в кожен нейрон повністю пов'язаного шару як вхідний. Кожен нейрон також має термін зміщення. Для цього шару є 16x10 входів, які всі спрямовані на кожен із 512 нейронів цього шару. Тому існують $(16 \times 10 + 1) \times 512$ відслідковуваних параметрів.

Для наступних двох шарів обчислення однакове: кількість параметрів = (кількість входів + зміщення) x кількість нейронів у шарі. Ось чому немає пояснення для повністю пов'язаних шарів 2 і 3.

Шар 5. Повністю з'єднаний №2:

- вхід: 512;
- вихід: 1024;
- кількість параметрів: 525312.

Шар 6. Повністю з'єднаний №3:

- вхід: 1024;
- вихід: 784 (що після переформатування повертає назад декодоване зображення розміром 28x28);
- кількість параметрів: 803600.

Загальна кількість параметрів у мережі: 8238608.

Висновки до розділу 3:

- у даному розділі був описаний капсульний метод, а саме: його відмінності від ЗНМ, основна концепція, що використовує вектори, які вказують функції об'єкта і називаються капсулами;
- була розглянута стійкість до змагальної атаки та точка зору інваріантності, це означає, що даний метод більш стійкий до змін в орієнтації і

розмірі введення, а також - потребує набагато менше даних для навчання, тому це може допомогти нейромережі розпізнавати один і той самий об'єкт;

- були розглянуті структура та обчислювальні етапи капсул, де капсули порівнювалися зі звичайними нейронами і були описані чотири етапи: матричне множення вхідних векторів, скалярне зважування вхідних векторів, сума зважених вхідних векторів та нова нелінійність між векторами;

- описана динамічна маршрутизація між капсулами, як нового алгоритму динамічної маршрутизації;

- описана архітектура КНМ, що складається з кодеру і декодеру.

Таким чином, проаналізувавши капсульний метод та його переваги над ЗНМ, у наступному розділі описується розроблена методика використання капсульного методу у задачах забезпечення безпеки ІС від НСД.

4 РОЗРОБКА МЕТОДИКИ ВИКОРИСТАННЯ КНМ В ЗАДАЧАХ ЗАХИСТУ ІС ВІД НСД

Згідно досліджень в рамках магістерської роботи, що наведені у розділах 3 та 4, КНМ в загальному використовують для задач автентифікації суб'єктів ІС. Але КНМ мають і інші варіанти застосування у задачах захисту ІС від НСД, а саме: розпізнавання об'єктів на зображеннях та відео, розпізнавання тексту та використання в ОПМ для розпізнавання кіберзагроз та класифікації типів шкідливого ПЗ.

4.1 Використання КНМ для розпізнавання об'єктів систем кібербезпеки

4.1.1 Використання КНМ для розпізнавання об'єктів чи осіб на зображеннях та відео

Розпізнавання об'єктів та осіб на зображеннях та відео може використовуватися для різних секторів захисту інформації.

У банківському секторі розпізнавання осіб використовується:

- у системах контролю доступу, для організації фізичного доступу в найбільш охоронювані приміщення і приміщення, в яких зберігаються цінності та грошові кошти;
- для ідентифікації, верифікації, автентифікації як фізично, так і програмних додатках;
- для підтвердження особи пред'явника паспорта і фото на паспорті.

Для правоохоронних органів розпізнавання осіб також може бути корисним. Сучасні системи розпізнавання осіб в змозі забезпечити не тільки виявлення злочинців, які перебувають у розшуку, або, наприклад, значаться зниклими, але забезпечують миттєве оповіщення, порушників, таким чином, допомагають здійснити оперативне реагування.

Відеоархів системи відеоспостереження зберігає і дозволяє при необхідності миттєво знайти інформацію про дату, час, напрямок руху цікавої людини, відеокадри із зображенням його особи. Межкамерний трекінг може відстежити подальший маршрут прямування злочинця після моменту виявлення.

Це може використовуватися на особливо охоронюваних об'єктах з пропускним режимом: міністерства і відомства, науково-дослідні інститути, медичні установи, промислові підприємства, школи, та ін.

Система розпізнавання осіб є ефективним інструментом для запобігання проникнення «небажаних» осіб на територію, що охороняється. До систем розпізнавання осіб на таких об'єктах можуть бути підключені як системи контролю доступу, які працюють в режимі верифікації, так і системи відеоспостереження які можуть в режимі моніторингу інформувати про попадання в об'єкти камери людей їх «чорного списку».

Капсульні мережі ефективні при розпізнаванні різних атрибутів певних об'єктів на зображенні, включаючи позу (положення, розмір, напрямок), деформацію, швидкість, відбивну здатність, відтінок, текстуру і т.д. Розпізнаючи зображення, КНМ можуть визначити, обличчя на зображенні чи ні. Здатність КНМ розпізнавати атрибути зображення залежить від характеристик капсул.

4.1.2 Використання КНМ у виявленні презентаційних атак в біометричних системах автентифікації

Революція в комп'ютерному обладнанні, особливо в блоках обробки графіки, дозволила досягти значного прогресу в комп'ютерній графіці та алгоритмах штучного інтелекту. На додаток до їх численних корисних застосувань у повсякденному житті та бізнесі, генеровані комп'ютером або маніпульовані зображення та відео можуть використовуватися для зловмисних цілей, що порушують системи безпеки, конфіденційність та соціальну довіру.

В контексті біометричних систем презентаційні атаки можуть називатися «атаками спуфінга». Відповідно до стандарту ISO/IEC 30107, атаки з використанням презентаційності визначаються як презентація підсистемі біометричного захоплення з метою втручання в роботу біометричної системи [16]. Ці атаки можуть бути атаками наслідування або обфускації. Атаки видачі себе за іншу особу намагаються отримати доступ, видаючи себе за когось іншого. Атаки обфускації можуть, наприклад, спробувати обійти системи виявлення та розпізнавання осіб.

Феномен діпфейку і його варіанти дозволяють звичайному користувачеві використовувати свій персональний комп'ютер, щоб легко створювати підроблені відео будь-кого з короткого реального онлайн-відео. Діпфейк – це зображення людини, що робиться за допомогою штучного інтелекту, тобто використовується накладення зображень чи відео, що існують на бажані зображення чи відео. Можуть бути введені кілька контрзаходів для боротьби з атаками, які використовують такі відео. Однак більшість із них націлені на певні домени, що робить їх неефективними при застосуванні до інших доменів або нових атак. У роботі [17] використовується КНМ, яка може виявляти різні види атак, від презентаційних атак з використанням друкованих зображень та відтворених відеороликів до атак з використанням фальшивих відео, створених за допомогою глибокого навчання. Також використовується набагато менше параметрів для навчання, ніж у традиційних ЗНМ з подібною продуктивністю.

4.1.3 Використання КНМ у виявленні людських дій на відео

Виявлення людських дій на відео також грає велику роль у безпеці ІС. Коректне та своєчасне розпізнавання людських дій може попередити фізичне викрадення інформації чи її носіїв, а також краще захистити об'єкт, де можуть розташовуватись ІС. Зараз використовується дуже багато камер спостереження з виявленням обличчя чи об'єктів на відео, тому виявлення людських дій може автоматизувати забезпечення безпеки об'єктів, що покращить їх захист.

Продемонстровані нещодавно досягнення у глибоких ЗНМ дали високі результати для відео класифікації людських дій, проте саме виявлення дій, як і раніше є складною проблемою. У роботі [18] була запропонована мережа 3D-капсул для відео, що називається VideoCapsuleNet: уніфікована мережа для виявлення дій, які можуть спільно виконувати піксельну сегментацію дій поряд із класифікацією дій. Запропонована мережа є узагальненням капсульної мережі від 2D до 3D, яка приймає послідовність відеокадрів на вході. Узагальнення 3D різко збільшує кількість капсул в мережі, що робить маршрутизацію капсул обчислювально дорогою. Було введено об'єднання капсул у згортковому шарі капсули для вирішення цієї проблеми, яке робить алгоритм голосування більш чутливим. Маршрутизація за домовленістю в мережі моделює уявлення про дії та їхні характеристики, що захоплені передбачуваними капсулами. Це може використовувати капсули для локалізації та виявлення специфічних для класу капсул у мережі, що звикли визначити піксельну локалізацію дій. Подальше вдосконалення локалізації можна зробити шляхом параметризованого пропуску з'єднань із згортковими шарами капсули, та навчати мережі наскрізним шляхом з класифікацією. Запропонована мережа досягає найсучаснішої продуктивності за кількох дій виявлення наборів даних.

Запропонована мережа приймає відеокадри як вхідні дані та передбачає клас дії та локалізацію пікселів для вхідного відеокліпу. Було запропоноване об'єднання капсул для оптимізації алгоритму голосування в згорткових шарах капсул, що робить маршрутизацію можливою. Запропонована мережа має компонент, який генерує піксельну локалізацію з урахуванням прогнозованої специфічної для класу капсули. VideoCapsuleNet можна навчити наскрізно і отримати найсучаснішу продуктивність на наборах даних з виявленням багатьох дій. Дослідження капсул все ще проводяться на початковому етапі, але вже можна побачити хороші результати з різних завдань. Основна ідея за капсулою інтуїтивно зрозуміла, і є багато фундаментальних причин, що робить капсули кращим підходом, ніж звичайні ЗНМ, однак, для повної перевірки цих

фактів знадобиться набагато більше досліджень. Ці результати є багатообіцяючими та вказують на потенціал капсул для відео.

4.2 Використання у ОПМ та аналізі тексту для розпізнавання кіберзагроз

4.2.1 Використання у ОПМ та аналізі тексту

ОПМ (обробка природної мови) – перетин машинного навчання і математичної лінгвістики, що спрямоване на вивчення методів аналізу і синтезу природної мови. Сьогодні ОПМ застосовується в багатьох сферах, в тому числі в голосових помічниках, автоматичних перекладах тексту і фільтрації тексту. Основними трьома напрямками є: розпізнавання мови, розуміння природної мови і генерація природної мови [19].

ОПМ - це ще одна область, де капсульні мережі можуть бути корисними. Протягом останніх років ЗНМ неодноразово застосовувався до розпізнавання мови, семантичного синтаксичного аналізу, класифікації речень та документів, машинного перекладу, синтезу звуку, моделювання мови та у подібних завданнях з обробки мови. Якщо структура мережі згортки з невеликою адаптацією дозволяє це зробити, то капсули також можна випробувати для таких цілей.

Капсульні мережі можуть бути гарним рішенням для проблем мовного моделювання, оскільки вони дозволяють вирішити деякі проблеми мереж згортки. Після шару згортки, як правило, слідує шар об'єднання, що є корисним для виявлення найважливіших особливостей. Однак максимальне об'єднання призводить до втрати інформації про структуру та взаємне розташування різних частин зображення. Тут можуть успішно працювати капсульні мережі. Такі нейронні мережі кращі там, де потрібно не тільки виділити якусь послідовність із цілого, але й врахувати порядок чи структуру окремих елементів. Хоча мережі згортки можуть бути корисними для таких завдань, як виявлення спаму, ідентифікації текстових сутностей або ключових ідей, КНМ може піти далі і

справлятися з ієрархічно складнішими завданнями, наприклад, аналізом шифру або виявленням помилок програми. Теоретично вони могли б бути кращими там, де існують високі вимоги до генерації мови. Перекладачі програм чат-ботів, пошукові системи та генератори вмісту можуть стати розумнішими за допомогою КНМ.

У ОПМ капсульний метод має більшу здатність ефективно засвоювати просторові відносини між словами, таких як місцевий порядок слів та їх семантичні уявлення. Було багато досліджень використання КНМ для завдань ОПМ, таких як аналіз настроїв, виявлення фальшивих новин, прогнозування продуктивності акцій за допомогою Twitter, неявне виявлення емоцій та образливі публікації в соціальній мережі. Результати цих досліджень показали, що КНМ перевершили ЗНМ у класифікації тексту.

Класифікація текстів - одне із основних і важливих завдань в області машинного навчання. Традиційно для представлення документів використовується терміни частота, зворотна частота документа, а для статистичної класифікації використовуються загальні класифікатори, такі як машини опорних векторів або логістична регресія.

Однак, останнім часом постійний розвиток методів глибокого навчання дозволив ефективно знаходити розподілені уявлення слів і документів, що в подальшому призвело до підвищення точності класифікації тексту. Основні моделі глибокого навчання, що використовуються при класифікації тексту, в значній мірі засновані на ЗНМ і зворотних нейронних мережах.

Тим часом, в області класифікації зображень капсульні мережі виявився ефективним для розуміння просторових відносин на високих рівнях даних за рахунок використання цілого вектора параметрів створення екземплярів. У статті [20] було застосовано цю мережеву структуру до класифікації тексту та стверджено, що вона також має переваги в цій області. Розпізнавання тексту може використовуватися задля аналізу даних соціальних мереж щоб виявляти кіберзагрози.

4.2.2 Розпізнавання кіберзагроз

Забезпечення безпеки програмного забезпечення, обладнання, даних та послуг стало важливою частиною управління будь-якою організацією через збільшення кількості нових атак, які загрожують її безпеці.

У кібербезпеці аналіз даних соціальних мереж став важливою областю досліджень через свої властивості надання оновлень про реальні події в реальному часі. Дослідження показують, що Twitter може містити інформацію про безпеку та загрози перед деякими спеціалізованими сайтами. Таким чином, класифікація твітів, пов'язаних з безпекою може допомогти з раннім попередженням таких атак.

Щоб бути готовими до кібератак, більшість організацій вдаються до інформації про безпеку та систем управління подіями для моніторингу своєї інфраструктури. Ці системи залежать від своєчасності та актуальності останніх оновлень, виправлень та загроз, що надаються інформаційними стрічками кіберзагроз. Інформаційні платформи з відкритим кодом, а саме мережі соціальних медіа, такі як Twitter, здатні об'єднати величезну кількість джерел, пов'язаних з кібербезпекою. Для обробки таких потоків інформації потрібні масштабовані та ефективні інструменти, здатні ідентифікувати та узагальнювати відповідну інформацію для зазначених активів. У дослідженні [21] було використано капсульний метод, як новий алгоритм глибокого навчання, і вперше досліджено в області безпеки виявлення атак через Twitter.

Метою було збільшити точність класифікації твітів за допомогою капсульної нейромережі, а не ЗНМ. Для досягнення мети дослідження, оригінальна реалізація КНМ з динамічною маршрутизацією пристосована для аналізу тексту за допомогою набору даних твітів. Для налаштування гіперпараметрів моделі був використаний метод довільного пошуку. Експериментальні результати показали, що капсульний метод перевищив базовий рівень ЗНМ за тим самим набором даних, з точністю 92,21% та 92,2%.

Набір даних містить твіти, отримані зі заздалегідь визначених облікових записів, пов'язаних із безпекою, в яких згадується відстежувана інфраструктура

або її активи, та позначаються як А, В та С. Використання спеціалізованих облікових записів Twitter усунуло отримання твітів, що містять потрібне ключове слово, без контексту безпеки, такі, як слова "apple, Windows, мережа, вірус, хробак, root". Набір даних уже був розділений на три набори: навчання, перевірка та тестування. Були використані два набори облікових записів спеціалістів з безпеки, позначені як S1 та S2. Набори навчання та перевірки містили твіти, отримані з облікових записів S1, тоді як набір тестувань складено з облікових записів S1 та S2. Метою використання різних наборів облікових записів Twitter було дати уявлення про ефективність моделей не лише на невидимих твітах, але й на твітах, отриманих з іншого набору облікових записів. Ще однією властивістю набору даних був часовий інтервал твітів, де набори перевірки та тестування отримувались з інтервалів часу, що слідували за навчальним набором. Це означає, що отримані результати імітували реальне розгортання моделі. Потім зібрані твіти були відфільтровані на основі набору ключових слів, що описують вибрані організації, і позначені безпечними чи ні.

4.3 Класифікація типів шкідливого ПЗ

Класифікація типів шкідливих програм є такою ж важливою, як і проблема виявлення шкідливого програмного забезпечення, оскільки ПЗ захисту системи розробляє свої стратегії щодо типів сімейства шкідливих програм. Родини шкідливих програм мають різну поведінку та вплив на комп'ютерну чи інформаційну систему. Кожне сімейство шкідливих програм використовує різні ресурси, файли, порти та інші компоненти операційних систем. Наприклад, зловмисне ПЗ в системах онлайн-банкінгу має на меті шахрайство, викрадення приватної інформації користувачів та використання різних способів розповсюдження.

Також, завдяки тенденціям розвитку технологій, нові типи шкідливих програм виникають майже щодня. Таким чином, більшість комп'ютерів, смартфонів та інших цифрових систем вразливі до нових шкідливих програм. У цьому випадку виконується багато атак нульового дня. Збільшення кількості шкідливих програм робить використання методів великих даних критичним для аналізу шкідливих програм.

Класифікація типу шкідливого програмного забезпечення є найпоширенішою проблемою в області кібербезпеки, оскільки стратегії систем захисту різняться щодо типу сімейства шкідливих програм. Проблема класифікації зловмисного ПЗ широко розглядається трьома різними способами: статичним, динамічним та на основі зображень. Останній перетворює зразки шкідливих програм в двомірні зображення в градаціях сірого, які можна аналізувати на основі їх унікальних критеріїв.

Класифікація типів шкідливого ПЗ на основі капсульного методу зосереджена на проблемі класифікації сімейства шкідливих програм на основі зображень. Однак класифікація типів шкідливих програм є незбалансованою задачею, тому це робить багато моделей невдалими в прогнозуванні рідкісних класів.

Поведінка шкідливого ПЗ різниться щодо типів шкідливого програмного забезпечення, що впливає на стратегії програмного забезпечення для захисту системи. Багато моделей класифікації шкідливих програм, що забезпечуються машинним або глибоким навчанням, досягають високої точності для прогнозування типів шкідливих програм. Моделі, засновані на машинному навчанні, повинні виконувати важкі інженерні роботи, що значно впливає на продуктивність моделей. З іншого боку, моделі глибокого навчання вимагають менших зусиль у розробці особливостей, порівняно з моделями машинного навчання. Однак традиційні компоненти архітектури глибокого навчання, такі як максимальне та середнє об'єднання, роблять архітектуру більш складною, а моделі більш чутливими до даних. Архітектури капсульних мереж, навпаки, зменшують вищезазначені складності, виключаючи компоненти об'єднання.

Крім того, моделі на основі капсульних мереж менш чутливі до даних, на відміну від класичних архітектур ЗНМ.

У роботі [22] пропонується модель мережевої КНМ, що заснована на техніці агрегування початкового завантаження. Запропонований метод випробуваний на двох широко використовуваних, незбалансованих наборах даних (Maling та BIG2015), для яких найсучасніші результати відомі і можуть бути використані для порівняння. Класифікація шкідливого ПЗ на основі капсульного методу є найсучаснішою технологією, яка піддається навчанню з меншою кількістю параметрів, ніж інші конкуренти.

4.4 Можливі напрями розвитку

Захист ІС від НСД є дуже важливим напрямком кібербезпеки у теперішні часи. Це пов'язано з тим, що атаки на кібермережі продовжують рости зі швидкістю, що випереджає здатність кіберзахисників писати та розгортати нові програми для виявлення цих нових атак. В поєднанні з досягненнями в розробці алгоритмів машинного навчання можна запропонувати багато можливостей застосування підходів КНМ до програм кібербезпеки для виявлення нових варіантів шкідливого ПЗ та атак нульового дня. Також капсульний метод може бути корисним у багатьох варіантах використання методів глибокого навчання, в тому числі і ЗНМ, для кібербезпеки, бо є вдосконаленням методу згортки, що використовується в ЗНМ. Хоча капсульний метод наразі є ефективним при розпізнаванні облич, що вже можна використовувати в задачах ідентифікації, автентифікації чи розпізнаванні відео, він також, як і описувалося в даному розділі, може використовуватися і в інших сферах.

Спеціалісти з кібербезпеки ще тільки шукають застосування для даного методу. Це пов'язано з тим, що системи безпеки дуже вимогливі, і їх вразливості можуть нанести велику шкоду ІС, її власникам і користувачам.

Тому, капсульний метод буде знаходити застосування у системах безпеки поступово, і йому треба деякий час, щоб зарекомендувати себе ефективним методом. Але після цього, КНМ можуть використовуватися багатьма організаціями, де використовуються ІС, для підвищення безпеки систем захисту. Різні конфігурації даної мережі будуть впроваджуватися в системах ідентифікації та автентифікації, системах відеомоніторингу приміщень, де знаходяться ІС, використовуючи можливості виявлення дій на відео, системах підвищення точності роботи антивірусного ПЗ, розпізнаючи та класифікуючи шкідливе ПЗ, системами Кіберполіції України чи спеціалістами з безпеки для виявлення кібератак.

Також, капсульний метод може розвиватись у виявленні ботнетів та розпізнаванні генерації доменних імен у великій кількості, які можуть бути використані зловмисником для важкого відстежування зв'язку із серверами [23]. Велика кількість різних доменних імен ускладнює блокування зловмисних доменів за допомогою стандартних методів, таких як створення чорного списку або загроза виявлення помилок. ЗНМ вже можуть використовуватися у даній сфері та покращувати існуючі методи, а капсульний метод є покращенням ЗНМ, тому впровадження його у існуючі системи розпізнавання може зробити їх більш ефективнішими.

Зараз майже всі користувачі ІС користуються мережею Інтернет і браузером для роботи, а зловмисники, в свою чергу, часто використовують вразливості браузера для зараження робочих комп'ютерів і системи в цілому. Використовуючи недоліки плагінів, зловмисник може перенаправляти користувачів з часто використовуваних веб-сайтів на веб-сайти, де експлойт-код змушує користувачів завантажувати та виконувати шкідливе програмне забезпечення. Такі типи атак називаються атаками завантаження. Наразі вже є запропоновані методи ЗНМ [23], які знизили експлуатаційні витрати на зараження шкідливим програмним забезпеченням і зменшили негативні наслідки доброякісних URL-адрес, які одночасно містяться на скомпрометованих веб-сайтах та переспрямовуються зі скомпрометованих веб-

сайтів. КНМ можуть показати значно вищі результати і в даному напрямку, тому це також можливий варіант розвитку цього методу.

Системи виявлення вторгнень у мережу мають важливе значення для забезпечення безпеки мережі від різних типів порушень безпеки. Вже існують побудовані алгоритми виявлення вторгнень, що використовують необроблені дані мережевого трафіку на основі згорткових нейромереж. Дані алгоритми класифікації вже дають дуже високу точність, порівняно із іншими нейромережними архітектурами чи іншими засобами, таким чином, КНМ можуть підвищити існуючі результати [23]. Окрім цього, ЗНМ досліджувалися і в характеристиці трафіку, що включає класифікацію типу мережного трафіку. Ідентифікація програми визначає, який тип програми використовується. Відзначається, що цей метод здатний розпізнавати зашифрований трафік та розрізняти трафік віртуальної приватної мережі та інший трафік. Тому капсули також можуть бути впроваджені і для цих задач.

Капсульний метод може запропонувати нові підходи до вирішення проблем кібербезпеки. Він зможе продемонструвати значні вдосконалення в порівнянні з традиційними системами, що базуються на підписах та на основі правил, а також класичними рішеннями на основі машинного навчання.

Висновки до розділу 4:

- було запропоновано впроваджувати КНМ у системи розпізнавання облич на фото та відео, що може використовуватися для ідентифікації та автентифікації;
- капсульний метод може використовуватися у виявленні презентаційних атак в біометричних системах автентифікації і задля виявлення людських дій на відео;
- дана методика пропонує використовувати капсульний метод для аналізу тексту та обробки природної мови для розпізнавання кіберзагроз на прикладі соціальної мережі Twitter;

- капсульний метод може бути впроваджено у класифікацію шкідливих програм;
- при розробці даної методики були проаналізовані можливі напрями розвитку капсульного методу для використання у захисті ІС від НСД, таких як розпізнавання та класифікація трафіку мережі, у виявленні ботнетів і генерації шкідливих доменних імен, при виявленні і зменшенні шкоди атак завантаження, і для виявлення вторгнень в ІС.

5 ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ТЕХНІЧНОЇ ЧАСТИНИ

5.1 Аналіз маркетингової частини проєкту забезпечення безпеки ІС від НСД на основі капсульного методу

Автоматизація та комп'ютеризація наразі є швидко зростаючою в Україні та світі. Тому забезпечення безпеки ІС є дуже важливим напрямом, що також розвивається. ШНМ – це одна з популярних наразі технологій, що використовуються у великій кількості різних областей, в тому числі, і в кібербезпеці. Штучні нейромережі зараз притягують багато інвестицій та з кожним днем стають все більш популярними і впровадженими у різні сфери нашого життя. Нейромережі все активніше використовуються у мобільних телефонах, ІС, КС, аналітиці, фотографії та ще у багатьох сферах. Але деякі існуючі ШНМ мають ряд недоліків, що може негативно впливати на розвиток описаних сфер. Саме тому був запропонований новий метод ШНМ, а саме - капсульний метод.

Таблиця 5.1 - Опис ідеї

Зміст ідеї	Напрямки застосування	Вигоди для споживачів (користувачів)
1	2	3
Капсульний метод штучних нейронних мереж може зробити більш швидкими та ефективніше автоматизованими різні напрями забезпечення безпеки ІС.	Банківський сектор.	Краща ідентифікація та автентифікація клієнтів або співробітників. Швидше та якісніше підтвердження особи. Ефективніший фізичний захист в найбільш охоронювані приміщення, де зберігаються цінності, цінні папери або гроші.

Продовження таблиці 5.1

1	2	3
Капсульний метод штучних нейронних мереж може зробити більш швидкими та ефективніше автоматизованими різні напрями забезпечення безпеки ІС.	2. Охорона.	Оперативне реагування. Краще розпізнавання порушників та злочинців. Система розпізнавання осіб є ефективним інструментом для запобігання проникнення «небажаних» осіб на територію, що охороняється. Також КНМ добре виявлять людські дії на відео, що допоможе автоматизувати процес охорони, що прискорить реагування.
	3. Особливо охоронювані об'єкти пропускним режимом.	Система розпізнавання осіб є ефективним інструментом для запобігання проникнення «небажаних» осіб на територію, що охороняється. До систем розпізнавання осіб на таких об'єктах можуть бути підключені як системи контролю доступу, які працюють в режимі верифікації, так і системи відеоспостереження які можуть в режимі моніторингу інформувати про попадання в об'єкти камери людей їх «чорного списку».

Кінець таблиці 5.1

1	2	3
	4. Соціальні мережі.	У кібербезпеці аналіз даних соціальних мереж став важливою областю досліджень через свої властивості надання оновлень про реальні події в реальному часі. Дослідження показали, що Twitter може містити інформацію про безпеку загрози перед деякими спеціалізованими сайтами. Таким чином, класифікація твітів, пов'язаних з безпекою, за допомогою КНМ, може допомогти з раннім попередженням про такі атаки.
	5. Антивірусне ПЗ.	Класифікація шкідливого ПЗ на основі капсульного методу є найсучаснішою технологією, яка піддається навчанню з меншою кількістю параметрів, ніж інші конкуренти. Також це прискорює та автоматизує роботу антивірусного ПЗ. Це робить антивірус, який використовує капсульний метод, ефективнішим та швидшим, ніж інші.

Основна ідея, що наведена у таблиці 5.1, у тому, що капсульний метод – це нова концепція у ШНМ, яка краще виконує задачі розпізнавання та класифікації, ніж інші нейромережі, наприклад, ЗНМ. КНМ можуть використовуватися у різних аспектах захисту ІС від НСД. Найпоширеніше

використання для розпізнавання осіб чи дій на фото та відео, що може застосовуватись для автентифікації. КНМ можуть бути корисні у виявленні презентаційних атак в біометричних системах автентифікації. Також КНМ можуть бути використані для аналізу тексту і розпізнавання кіберзагроз у соціальних мережах та в класифікації типів шкідливого ПЗ. Тому, задля забезпечення безпеки ІС, можна виділити такі базові потенційні ринки використання капсульного методу: банківська сфера та усі об'єкти, де потрібна охорона: міністерства і відомства, науково-дослідні інститути, медичні установи, промислові підприємства, школи, та ін. Також, цей метод може автоматизувати роботу Кіберполіції України у аналізі даних, що можуть бути пов'язані з безпекою, в соціальних мережах. Також цей метод може бути застосований у класифікації типів шкідливого ПЗ, що може використовуватися ІТ-компаніями, які розробляють антивірусне ПЗ. Тобто, основними потенційними клієнтами можуть бути банки, компанії, що надають послуги охорони та ІТ-компанії, що розробляють антивірусне ПЗ.

Так як капсульний метод може бути широко застосований у різних сферах кібербезпеки, треба детальніше охарактеризувати потенційний ринок в Україні, що наведено у таблиці 5.2.

Таблиця 5.2 - Попередня характеристика потенційного ринку

№	Показники стану ринку (найменування)	Характеристика
1	2	3
1.	Головні конкуренти	ІТ-компанії
		Компанії, що надають охоронні послуги
		Банки
2.	Динаміка ринку (якісна оцінка)	Стагнує
3.	Наявність обмежень для входу (вказати характер обмежень)	Потребує великих інвестицій

Кінець таблиці 5.2

1	2	3
4.	Специфічні вимоги до стандартизації сертифікації	Треба розробляти специфічні сертифікації та стандартизації

Тобто, як видно з таблиці 5.2, даний ринок стагнує, тому що ніхто в Україні не використовує на даний момент капсульний метод штучний нейронних мереж для задач безпеки ІС. Тому, основними конкурентами можуть бути ІТ-компанії, що можуть почати використовувати цей метод, компанії, що надають охоронні послуги та банки. Але так як цей метод тільки набирає оберти, він потребує значних інвестицій та розробки специфічних стандартизацій та специфікацій. Тобто зайти на ринок з цією технологією, з одного боку, не складно, бо ніхто ще її не використовує, але і важко, бо це потребує великих інвестицій.

Тому, для детального визначення потенційних груп клієнтів, їх характеристики, та формування орієнтовного переліку вимог до даного методу для кожної групи, було зроблено таблицю 5.3.

Таблиця 5.3 – Попередня характеристика потенційних клієнтів

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів (користувачів)
1	2	3	4	5

Продовження таблиці 5.3

1	2	3	4	5
1.	Захист об'єктів.	Охоронні організації.	Міністерства і відомства – ефективність, налаштування під потреби, швидкість роботи. Науково-дослідні інститути – налаштування під власні потреби, ефективність. Медичні установи та підприємства – налаштування під специфічні задачі, простота використання, вартість, ефективність. Школи та інші установи – простота введення та використання, вартість, ефективність.	Ефективність та швидкість заходів забезпечення безпеки. Налаштування під особливі потреби.

Кінець таблиці 5.3

1	2	3	4	5
2.	Захист даних та цінностей банків.	Банки.	Фізичні банки – налаштовуваність під особливі потреби, ефективність, стійкість до атак та взлому, швидкість роботи. Мобільні банки – ефективність, стійкість до атак, швидкість роботи, налаштовуваність під потреби.	Ефективність, швидкість та надійність заходів забезпечення безпеки, стійкість до атак. Налаштовуваність під особливі потреби.
3.	Захист комп'ютерів або мобільних пристроїв від шкідливого ПЗ.	ІТ-компанії.	Компанії, що розробляють антивірусне ПЗ – вартість, ефективність, інноваційність, легкість введення. Компанії, що розробляють різне ПЗ – вартість, ефективність, легкість впровадження та підтримки, налаштування під потреби.	Інноваційність, ефективність та вартість заходів забезпечення безпеки, легкість впровадження, налаштування під потреби.

Із таблиці 5.3 можна зробити висновок, що для користувачів сфер захисту банку, об'єктів та комп'ютерів або мобільних пристроїв важливі ефективність, надійність, швидкість методів забезпечення безпеки, вартість,

легкість впровадження і підтримки, а також – налаштування під особливі потреби.

Для визначення сильних та слабких сторін використання капсульного методу штучних нейронних мереж, був здійснений SWOT-аналіз середовища реалізації інноваційного проекту, що наведений у таблиці 5.4

Таблиця 5.4- SWOT-аналіз

Сильні сторони:	Слабкі сторони:
- Інноваційність; - порівняна ефективність забезпечення захисту; - висока інтегрованість у різні сфери; - відсутність аналогів на ринку; - доступність технології.	- Недопрацьованість технології, як нової; - потребує специфічних спеціалістів для реалізації; - низька розповсюдженість методу; - неможливість використання одразу, потрібен час для тестувань.
Можливості:	Загрози:
- Може використовуватись у багатьох сферах; - залучення інвестицій; - висока конкуренція серед аналогічних пропозицій; - великий потенціал розвитку методу; - буде більш доступний з часом.	- Може зайняти багато часу для впровадження; - не буде достатньої кількості спеціалістів (кваліфікованих кадрів); - великі витрати праці спеціалістів; - може з'явитися більш доступна та продуктивна технологія; - міжнародний ринок витіснить український потенціал.

Також, щоб більш розгорнуто розглянути капсульний метод, треба розробити ринкову стратегії проекту. Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів, що описано в таблиці 5.5.

Таблиця 5.5 - Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивніс ть конкуренції в сегменті	Простота входу у сегмент
1	2	3	4	5	6
1.	Власники об'єктів, що потребують охорони	У найближчий час не дуже велика готовність, бо метод ще новий.	Низький попит, тому що існуючі методи розвинені.	Конкуренці я досить велика, тому що існує багато охоронних служб, які надають свої послуги.	Складно, тому що охоронні заходи та засоби потребують випробувань на надійність.
2.	Власники банків	У найближчий час не дуже велика готовність, бо метод ще новий.	Низький попит, тому що існуючі методи розвинені та на даний момент можуть бути ефективніши ми і дешевшими.	Велика, тому що банків багато, але через специфічніс ть умов, що потрібні, конкуренція не така велика, як у 1 цільової групи.	Дуже складно, тому що заходи та засоби для забезпеченн я безпеки банку – дуже серйозне завдання.

Кінець таблиці 5.5

1	2	3	4	5	6
3.	Власники ІТ-компаній	У найближчий час не дуже велика готовність, бо метод ще новий.	Низький попит, але ІТ-компанії можуть швидше впроваджувати нові технології, ніж інші сектори.	Велика, тому що ІТ-компаній багато в Україні, але мало хто з них розробляє антивірусне ПЗ. Тому саме у ринку таких компаній конкуренція менша.	Середня складність, тому що можна достатньо легко створити свій стартап або створити свою ідею в ІТ.
Які цільові групи обрано: Власники ІТ-компаній, тому що на цей ринок можна легше зайти та швидше впровадити ідею.					

Тепер потрібно ідентифікувати стейкхолдерів, здійснити їх пріоритизацію та побудувати карту стейкхолдерів, яка дозволить візуалізувати картину взаємозв'язків стейкхолдерів. Вона позначена на рисунку 5.1.

Створення карти проводилось у 4 етапи:

1) ідентифікація – окреслення актуальних груп стейкхолдерів. Це ІТ-компанії, бізнес-партнери, держава, інвестори, фіскальна служба, споживачі, міжнародні організації та наукові організації та установи;

2) аналіз – дослідження впливу та інтересів стейкхолдерів;

3) візуалізація – візуальна ілюстрація взаємодії зі стейкхолдерами;

4) пріоритезація – вибір ключових стейкхолдерів, які найкраще

відповідали б істотним питанням, визначеним на попередньому етапі.

З метою відображення взаємозв'язків стейкхолдерів на карті на рисунку 5.1 виокремлено три концентричних області, в яких розміщено всіх зацікавлених осіб інноваційного проекту за можливостями впливу на них ініціатора проекту. Область внутрішніх стейкхолдерів – область повноважень або відповідальності ініціатора. Внутрішні зацікавлені сторони знаходяться в прямій підлеглих ініціатора, що дозволяє використовувати досить прості методи адміністрування проекту.

Залежні зацікавлені сторони формально ініціатору проекту не підлеглі, проте тісні ділові стосунки потребують на пошук взаємовигідних рішень та компромісів. На периферії ж знаходяться зовнішні зацікавлені сторони. Це область стейкхолдерів опосередкованого впливу на успішність реалізації інноваційного проекту.

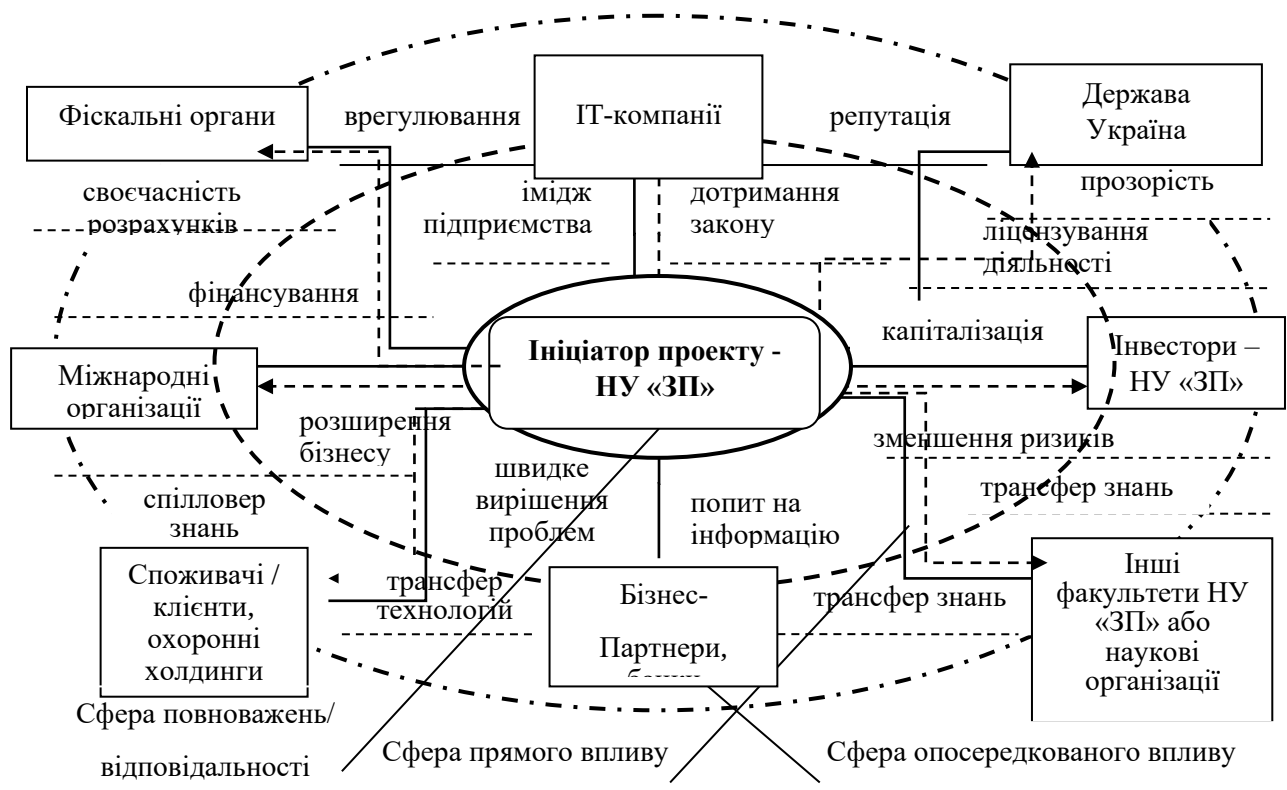


Рисунок 5.1 – Карта стейкхолдерів

5.2 Визначення витрат на аналіз капсульного методу для забезпечення безпеки ІС від НСД

Розрахунок заробітної плати працівників виконується на основі погодинної тарифної ставки виконуючих робіт, додаткової заробітної плати у вигляді премії (10-15%) на 90 днів, яких потрібно для аналізу методу капсульних нейромереж для забезпечення безпеки ІС від НСД, а також ЄСВ. Єдиний соціальний внесок дорівнює 22% від основної та додаткової заробітної плати. Склад, чисельність та фонд заробітної плати виробничих працівників наведений у таблиці 5.6.

Таблиця 5.6 - Склад, чисельність та фонд заробітної плати виробничих працівників

Категорії працівників	Наявна чисельність, осіб		Тарифна ставка за розрядом виконуваних робіт, грн / годину	Ефективний фонд робочого часу, годин	Тарифний заробіток у міс., грн.	Преміальний відсоток до тарифного заробітку	Розмір премії в місяць, грн.	Фонд заробітної плати за 90д., грн.	ЄСВ у місяць, грн.
	за зміну	на добу							
1	2	3	4	5	6	7	8	9	10

Кінець таблиці 5.6

1	2	3	4	5	6	7	8	9	10
Виробничі працівники, в тому числі: 1.Основні працівники (молодший науковий співробітник)	1	0	50	720	8000	10	800	36000	1936
2.Допоміжні працівники (науковий керівник)	1	0	65	720	10400	15	1560	46800	2631,2
3.Черговий та ремонтний персонал (лаборант)	1	0	35	720	5600	10	560	25200	1355,2
Разом виробничих працівників	3	0	X	X	X	X	2920	10800 0	5652,4

Для аналізу забезпечення безпеки ІС від НСД на основі капсульного методу необхідно спеціальне обладнання: 2 ЕОМ Asus X509FJ-BQ039, 2 маніпулятори типу миша та принтер HP LaserJet Pro M132A.

Розрахунок можливих транспортно-заготівельних витрат визначається як 5% від вартості матеріалів. Витрати на матеріали для аналізу наведені в таблиці 5.7.

Таблиця 5.7 – Розрахунок матеріальних витрат

Матеріальні витрати	Норматив у розрахунку на один. продук. (послуг)	Виробнича програма	Обсяг сировини	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
ЕОМ Asus X509FJ-BQ039	2	-	2	14000	28000
Миша Logitech M170 Wireless	2	-	2	150	300
Принтер HP LaserJet Pro M132A	1	-	1	16000	16000
Ручка	3	-	3	10	30
Картридж для принтера	1	-	1	600	600
Папір формату А4 для принтера	1	-	1	400	400
USB Flash накопичувач об'ємом 16Gb	1	-	1	500	500
Транспортно-заготівельні витрати	-	-	-	-	76,5
Разом	-	-	-	-	45890

При аналізі капсульного методу ШНМ були спожиті такі послуги як: електропостачання, водопостачання, а також – теплопостачання. Площа приміщення, де проходить аналіз, дорівнює 35м². Розрахунок вартості спожитих послуг внесено до таблиці 5.8.

Таблиця 5.8 – Розрахунок вартості спожитих послуг

Вид послуг	Норматив у розрахунку на один. продук. (послуг)	Виробнича програма	Обсяг послуг	Тарифи	Сума, грн
1	2	3	4	5	6
Електропостачання	T1	100%	100 кВт	2,68 грн/ кВт	268
Водопостачання	B1	100%	10 м ³	5,688 грн./м ³	56,88
Теплопостачання	TE	100%	35,0 м ²	39,21 грн/м ²	1372,35
Разом	-	-	-	-	1697,23

Амортизація була розрахована як первісна вартість, що поділена на допустимий строк корисного використання спеціального обладнання, що складає 3 роки.

Таким чином розрахована сума амортизації для ЕОМ Asus X509FJ-BQ039 та принтера HP LaserJet Pro. Результати розрахунків внесено до таблиці 5.9.

Також мною була розрахована балансова (залишкова) вартість основного засобу, що дорівнює різниці між первісною (переоціненою) вартістю об'єкта та сумою накопиченої амортизації та накопичених збитків від зменшення його корисності, а також – витрати на поточний ремонт, що дорівнюють 2% від балансової вартості.

Балансова вартість досягає нуля, коли первісна вартість об'єкта дорівнює сумі накопиченої амортизації та збитків від зменшення його корисності.

Балансова вартість: $37150 - 17166 = 19984$ грн.

Витрати на поточний ремонт = $19984 \times 0,02 = 399,7$ грн.

Таблиця 5.9 – Розрахунок амортизації

Група основних засобів	Норма амортизації	Первісна вартість ОЗ на 01.01	Надійшло ОЗ		Вибуло ОЗ		Сума грн
			дата	пер. вар.	дата	пер. вар.	
1	2	3	4	5	6	7	8
EOM Asus X509FJ-BQ039	33%	31000	10.11. 2020	31000	-	-	10333
Принтер HP LaserJet Pro M132A	33%	20500	10.11. 2020	20500	-	-	6833
Разом		37150		37150		-	17166

Брутто-інвестиції складаються з вільних грошових коштів (прибутку, амортизації необоротних активів та ін.). За своєю економічною природою вони більше тяжіють до активно-пасивним інвестицій, так як спрямовані на придбання нового обладнання, ресурсозберігаючих технологій, створення власними силами нових основних засобів (фондів), заміну застарілого обладнання, модернізацію, а також диверсифікацію капіталу [24].

Для даного проєкту брутто-інвестиції можуть бути корисними та важливими, тому що метод капсульних ШНМ швидко розвивається, і обладнання може через швидкий час стати застарілим для проведення аналізу або використання.

У даній роботі проводиться аналіз капсульного методу для забезпечення безпеки ІС, тому визначити собівартість даної послуги визначається як повна собівартість, що включає в себе витрати на матеріали, обладнання, заробітну плату, ЄСВ, витрати на спожиті послуги, амортизацію, а також – на ремонт. Кошторис усіх витрат розраховано у таблиці 5.10.

Таблиця 5.10 – Кошторис витрат

Калькуляційні статті	Витрати	
	у розрахунку на одиницю продукції, грн.	у розрахунку на весь обсяг продукції, грн.
1	2	3
Сировина та матеріали	366	1830
ЕОМ Asus X509FJ-BQ039	14000	28000
Принтер HP LaserJet Pro M132A	16000	16000
Електропостачання	268	268
Водопостачання	56,88	56,88
Теплопостачання	1372,35	1372,35
Інші	76,5	76,5
Разом	-	47603,73
Заробітна плата основних виробничих працівників за 90 д.	40380	121140
ЄСВ 22% за 90 д.	8883,6	26650,8
Амортизація за 3 міс.	5722	17166
Витрати на утримання та експлуатацію основних засобів поточний ремонт	133,3	399,7
Загальновиробничі витрати	-	21169,5
Виробнича собівартість	-	218591,35

Кінець таблиці 5.6

1	2	3
Адміністративні витрати	-	-
Інші витрати	-	-
Повна собівартість	-	218591,35

Для даного проєкту наразі складно визначити дохід, тому що результати роботи є у вигляді аналізу, в який сферах і яким чином може використовуватись капсульний методі штучних нейромереж для захисту ІС від НСД. Це пов'язано з тим, що впровадження даного методу може бути у різні сфери кібербезпеки з різною специфікою, і тому їх вартість може сильно відрізнятись в залежності від цього. Але через покращення безпеки ІС цим методом зростає ступінь захисту системи, що призводить до удосконалення експлуатаційних витрат і до економії. Розрахунок економії проводився за формулою 5.1:

$$E = B. \text{ собівартість} \times k - H. \text{ собівартість}, \quad (5.1)$$

де E – економія, грн;

$B. \text{ собівартість}$ – базова собівартість, грн;

k – коефіцієнт експлуатації ресурсу;

$H. \text{ собівартість}$ – нова собівартість проєкту, грн.

Припустимо, що базова собівартість – а саме собівартість аналізу забезпечення безпеки ІС від НСД без капсульного методу дорівнює 192000 грн., тому що дані методи вже використовуються, і про них є багато інформації, тому часу і ресурсів для цього треба менше, а коефіцієнт експлуатації ресурсу – 1,4.

Таким чином, підставивши усі значення у формулу 5.1, отримаємо:

$$E = 192000 \times 1,4 - 218591,35 = 50208,65 \text{ (грн)}.$$

З даного розрахунку можна зробити висновок, що використання капсульного методу принесе 50208,65 грн. економії, завдяки тому, що цей аналіз покращує безпеку ІС, що робить системи більш довговічними та стійкішими до різних атак, які, в свою чергу, можуть призвести до додаткових витрат.

У даному розділі дипломного проєкту були визначені маркетингові аспекти, а саме: описана ідея, проведена попередня характеристика потенційного ринку та клієнтів, зроблений SWOT-аналіз, обрані групи потенційної цільової аудиторії, а також складена карта стейкхолдерів. Також, була розрахована собівартість на 90 днів реалізації проєкту, що складає 218591,35 грн. з урахуванням річної заробітної плати молодшого наукового співробітника, його керівника і лаборанта, та їх ЄСВ. Також, були розраховані вартість спожитих послуг, в тому числі і специфічного обладнання, а також – амортизація до нього за 3 місяці. Була розрахована економія від аналізу капсульного методу нейромереж для забезпечення безпеки ІС від НСД, яка складає 50208,65 грн.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Аналіз потенційних небезпек

У даному розділі дипломного проєкту розглядаються заходи з охорони праці та безпеки під час виникнення надзвичайних ситуацій у виробничих приміщеннях, де можуть використовуватися капсульні нейронні мережі для захисту інформаційних систем.

Повністю безпечних та нешкідливих умов праці не існує. Виробниче середовище завжди характеризується наявністю певних небезпечних та шкідливих для здоров'я людини чинників. Саме тому, питанням охорони праці з кожним роком приділяється все більше уваги.

У даній роботі проводиться аналіз капсульного методу для забезпечення безпеки ІС від НСД. При проведенні аналізу, який представлений в даній роботі, відбувається безпосередній контакт з комп'ютером. Постає питання про те, як має бути організоване робоче місце, щоб знизити професійний стрес, збільшити продуктивність і ефективність роботи, а також створити сприятливі і комфортні робочі умови.

Дослідження робочого місця проводилось у кабінеті програмування, де повинні бути передбачені заходи захисту від можливого впливу небезпечних і шкідливих факторів виробництва. Рівні цих факторів не повинні перевищувати граничних значень, обумовлених правовими, технічними і санітарно-технічними нормами.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою. Тож постійне використання комп'ютера в процесі роботи пов'язано безпосередньо з наступними факторами, що чинять негативний вплив на організм:

- підвищена чи знижена температура повітря;
- надмірна запиленість чи загазованість повітря;
- підвищена чи знижена вологість повітря;
- недостатня освітленість робочого місця;
- перевищення допустимих норм шуму;
- підвищений рівень іонізуючого випромінювання;
- підвищений рівень електромагнітних полів;
- підвищений рівень статичної електрики;
- бляклість екрану дисплея.

Крім того, на користувачів комп'ютерів діє ряд факторів малої інтенсивності, негативні ефекти яких проявляються поступово і таємно. Тому хвороби з'являються тільки після багатьох місяців або навіть років роботи, коли з ними вкрай складно боротися. У багатьох випадках складно навіть встановити першопричину захворювання. В таких умовах виникає необхідність формувати у майбутніх фахівців актуальні знання про вплив несприятливих виробничих факторів на робочому місці за допомогою інформаційних технологій, заходів та інструментів, спрямованих на мінімізацію такого впливу, збереження здоров'я і професійного довголіття користувачів.

6.2 Заходи по забезпеченню техніки безпеки

Згідно з «Правилами улаштування електроустановок» з електробезпеки кабінет програмування відноситься до приміщень підвищеної небезпеки, так як потенційно можливий випадок одночасного дотику людини до металевих корпусів електричних пристроїв і заземленим металевим конструкціями будівлі. Наприклад, може статися так, що людина однією рукою схопить за батарею, а іншою - за корпус персонального комп'ютера.

Щоб уникнути ризику поразки електричним струмом при контакті з металевими неспровідними деталями, які можуть виявитись під напругою із-за

пошкодження ізоляції, відповідно до ДСТУ 7237: 2011 «Система стандартів безпеки праці. Електробезпека. Загальні вимоги та номенклатура видів захисту» прийняті наступні захисні заходи: вирівнювання потенціалів, створення захисного заземлення, застосування систем наднизького напруження та автоматичне відключення живлення, а також захисне розділення електричних кіл.

Для запобігання ураження електричним струмом згідно з НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів» струмопровідні частини лабораторного обладнання, які є джерелами небезпеки, надійно ізольовані і перебувають у недоступних для людей місцях [25]. Таким чином, у кабінеті організовано захисне заземлення експлуатаційного обладнання та його занулення (ДСТУ 7237:2011) задля захисту людини від ушкодження електричним струмом при дотику до неструмопровідних частин, які внаслідок пошкодження ізоляції опинилися під напругою. Заземлення виводиться за допомогою мідного кабелю, який з'єднаний з мідною шиною, що пов'язана зі земляним контуром будівлі.

Комп'ютери, сервери, джерела безперебійного живлення, принтери, копіювальні апарати, що знаходяться в досліджуваному приміщенні, живляться від мережі 220 В. Технічний огляд всього обладнання і електропроводки в офісі проводиться систематично. Дозволяється працювати тільки на працюючих комп'ютерах і забороняється самостійний ремонт несправної проводки та іншого обладнання. У комп'ютерний кабінет допускаються тільки особи, що пройшли інструктаж. Згідно з НПАОП 0.00-4.12-05, затвердженого наказом Голови Державного комітету України по нагляду в сфері охорони праці від 26.01.2005 № 15, посадові особи проходять навчання і перевірку знань з охорони праці, при прийомі на роботу і один раз на три роки проходять навчання відповідно до Типового тематичного плану і програмою навчання з охорони праці посадових осіб [26].

Для захисту робітників кабінету від ураження електричним струмом застосовуються як організаційні, так і технічні засоби захисту.

Для організації та дотримання електробезпеки в виробничому приміщенні всі робітники дотримуються правил охорони праці при експлуатації електро-обчислювальних машин, що затверджені в НПАОП 0.00-1.28-10. Комп'ютерні робітники мають I кваліфікаційну групу з електробезпеки, яка присвоюється персоналу, який не має відношення до електрики, тобто особам, які не мають спеціальної електротехнічної підготовки. Адміністратор приміщення має II кваліфікаційну групу з електробезпеки, так як кваліфікаційна комісія присвоює її електротехнічному персоналу, який обслуговує установки і обладнання з електроприводом.

Організаційні заходи, які проводяться в кабінеті:

- призначення осіб, відповідальних за організацію та безпеку виконання робіт;
- навчання персоналу правилам виконання робіт та експлуатації електротехнічного обладнання;
- оформлення наряду або розпорядження на проведення робіт;
- проведення інструктажів перед початком робіт з електроустановками;
- організація нагляду за проведенням робіт;
- встановлення раціональних режимів праці та відпочинку;
- застосування засобів індивідуального захисту, попереджувальних плакатів і знаків безпеки відповідно до вимог ДСТУ ISO 7010:2009 [27].

До технічних заходів, які проводяться в кабінеті, відносять:

- електричний поділ мережі;
- компенсація струмів замикання на землю згідно з (ГКД 34.20.172-95);
- вирівнювання потенціалу (ДСТУ 2815-94);
- застосування захисного заземлення, занулення;
- контроль і профілактика ізоляції;
- захисне відключення (ДСТУ HD 62640:2016).

Також в комп'ютерному приміщенні для запобігання виникнення нещасних випадків є обов'язковим дотримання наступних правил:

- забороняється передавати електрообладнання особам, які не мають права працювати з ним;
- забороняється використовувати вилки, розетки, проводи з пошкодженою ізоляцією;
- забороняється залишати без нагляду ввімкнену техніку, при перерві в роботі і по закінченню робочого дня необхідно вимикати всю техніку, яка підключена до мережі;
- забороняється використовувати несправне обладнання (перед початком зміни потрібно перевірити все використовуване обладнання);
- забороняється наступати на дроти, які лежать на підлозі.

6.3 Заходи з виробничої санітарії та гігієни праці

Заходи щодо забезпечення виробничої санітарії і гігієни праці розробляються відповідно до вимог Державних санітарних норм та правил «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу», МІОУ 06.05.2014 р. за № 472/25249 (далі – «Гігієнічна класифікація праці»). Гігієнічна класифікація праці базується на оцінці її умов залежно від фактично визначених рівнів впливу факторів виробничого середовища і трудового процесу з урахуванням їх можливої шкідливої дії на здоров'я працівників. Оцінка умов праці на робочих місцях, аналіз впливу на працюючих санітарно-гігієнічних чинників і параметрів трудового процесу, передбачених гігієнічною класифікацією проводиться в процесі трудової діяльності. При цьому, оцінюється технічний і організаційний рівень робочого місця та ступінь можливого ушкодження здоров'я.

Кабінет знаходиться на п'ятому поверсі одинадцятиповерхового цегляного будинку, що відповідає нормам ДСанПіН 3.3.2-007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [28].

Параметри приміщення становлять: довжина $A = 7$ м, ширина $B = 5$ м, висота $H = 3$ м. Загальна площа кімнати дорівнює $S = 35$ м², а об'єм $V = 105$ м³. В кабінеті працює не більше 4 осіб. Тож площа і об'єм приміщення, що припадає на одного співробітника дорівнює відповідно 8,75 м² та 26,25 м³ відповідно. Такі параметри відповідають допустимим нормам вказаних у ДСанПіН 3.3.2-007-98. Приміщення містить системи телефонії, комп'ютеризації та сигналізації.

Для внутрішнього оздоблення інтер'єру приміщення використані дифузно-відбивні матеріали з коефіцієнтом відбиття для стелі 0,7, для стін 0,6. Покриття підлоги кабінету є матовим з коефіцієнтом відбиття 0,4. Поверхня підлоги рівна, неслизька, з антистатичними властивостями. Стіни кабінету пофарбовані в білий колір. Приміщення обладнані шафами для зберігання документів, полицями. Щоденно проводиться вологе прибирання кабінету, а також систематично відбувається провітрювання кабінету. Таким чином, приміщення відповідає існуючим санітарним нормам.

Одним з головних засобів відображення інформації і однією з основних складових частин ПК є дисплей. Дисплей розміщений на столі так, щоб відстань спостереження інформації на екрані не перевищувало 700 мм від очей користувача. Висота робочої поверхні столів становить 80 см. Клавіатура розташовується на підставці на відстані 100 - 300 мм від краю, направлено до користувача, для того щоб його положення рук було паралельно підставці, а кисті були розташовані над поверхнею на висоті не більше 20-35 мм при роботі на клавіатурі. Це положення дозволяє розслаблятися рукам в перервах між роботи із ПК, і не напружує кисті та передпліччя.

Кожне робоче місце розташоване в кабінеті по периметру так, що природне світло попадає на монітори ліворуч або праворуч від працівника.

Приміщення обладнано системою загального рівномірного освітлення, люмінесцентні лампи типу ЛД потужністю 20 Вт розташовані на стелі в ряд таким чином, щоб напрямок штучного й природнього світла співпадали. Завдяки цьому рівень освітленості за робочим місцем дорівнює близько 200 лк. Крім загального освітлення, на кожному робочому місці встановлені додаткові локальні світильники.

Для перевірки відповідності рівня освітлення в кабінеті нормативним вимогам зазначених у ДБН В.2.5-28-2018 необхідно провести розрахунок оцінки штучної освітленості кабінету. Для цього застосуємо метод коефіцієнта використання світлового потоку, який використовують при розрахунку загального рівномірного освітлення горизонтальних поверхонь з урахуванням відбитих від стін, підлоги і стелі світлових потоків [29]. Згідно з державних будівельних норм України ДБН в.2.5–28:2018 "Природне і штучне освітлення" дане приміщення відноситься до розряду зорової роботи III г з високою точністю зорової роботи, а також нормативною мінімальною освітленістю виробничого приміщення у 200 лк. Як джерело світла був обраний ЛПО світильник зі ступенем захисту IP20, що захищений від твердих часток розміром понад 12 мм і не має захисту від вологи. А також з коефіцієнтами відбиття поверхонь приміщення $\rho_c=70\%$; $\rho_{ст}=50\%$; $\rho_{п}=30\%$.

Загальна освітленість приміщення визначається за наступною формулою:

$$E_p = \frac{\Phi_l N_{\phi l} \cdot \eta}{S \cdot k_z \cdot z}, \text{ лк} \quad (6.1)$$

де E_p – загальне освітлення в приміщенні;

$N_{\phi l}$ – фактична кількість ламп, яке дорівнює 18;

Φ_l – світловий потік лампи, дорівнює 1100 лм;

S – площа приміщення, що освітлюється, дорівнює 35 м²;

z – коефіцієнт нерівномірності освітлення для люмінесцентних ламп, дорівнює 1,1;

k_3 – коефіцієнт запасу, що враховує зниження освітлення через забруднення та старіння лампи, приймаємо, що він дорівнює 1,3;

η – коефіцієнт використання освітлювальної установки, 0,51.

Щоб визначити η потрібно знайти індекс приміщення i за наступним виразом:

$$i = \frac{AB}{h(A+B)}, \quad (6.2)$$

де A – довжина приміщення, м;

B – ширина приміщення, м;

h – висота розміщення світильників над робочою поверхнею, м.

Висота розміщення світильників над робочою поверхнею h входить до загальної висоти приміщення, яка визначається за формулою 6.3:

$$H = h + h_p + h_3, \text{ м} \quad (6.3)$$

де H – висота виробничого приміщення, м;

h_p – висота робочої поверхні над підлогою, що дорівнює 0,8 м.

h_3 – висота звисання світильника від стелі, м.

Для знаходження h і h_3 треба розрахувати кількість рядів світильників у приміщенні за формулою 6.4, а результат округлити до найбільшого цілого:

$$N_p = \frac{B}{(H - h_p) \cdot [L/h]}, \quad (6.4)$$

де $[L/h]$ – числове значення коефіцієнта світильника, яке дорівнює 1,4.

$N_p = 2$. А далі потрібно знайти максимально припустиму відстань між рядами світильників, яка дорівнює 2,5 м. Таким чином, h дорівнює як максимальна припустима відстань між рядами світильників поділена на коефіцієнт світильника, що буде складати 1,8.

Підставивши значення в формулі 6.2 6.3 дані значення, отримаємо наступні показники:

$$h_3 = H - h_p - h, \quad (6.5)$$

$$i = \frac{7 \times 5}{1.8 \times (7+5)} = 1,62.$$

Враховуючи світлі відтінки стін, стелі й поверхні підлоги, тип світильника стельової установки, а також отримане значення індексу приміщення i визначимо, що коефіцієнт використання освітлювальної установки $\eta = 0,51$.

Далі потрібно визначити сумарний світловий потік освітлювальної установки у даному виробничому приміщенні за формулою 6.6:

$$\Phi_{\Sigma} = \frac{E_n \cdot S \cdot k_3 \cdot z}{\eta}, \quad (6.6)$$

де Φ_{Σ} – розрахункове значення сумарного світлового потоку у приміщенні, лм;

E_n – нормоване значення освітленості, лк;

S – площа освітлюваної поверхні, м²;

k_3 – коефіцієнт запасу;

z – коефіцієнт нерівномірності (мінімальної) освітленості;

η – коефіцієнт використання світлового потоку.

Підставивши усі значення у формулу 6.6, знайдемо Φ_{Σ} , який дорівнює 19627,5 лм. Також була визначена розрахункова загальна кількість світильників у приміщенні, виходячи з позиції розташування їх у вершинах квадрата: 6. І завдяки цьому був визначений розрахунковий світловий потік лампи $\Phi_{\text{л}}^*$, який дорівнює 1090 лм. Найближчий до нього фактичний світловий потік це світловий потік ЛТБ лампи, який дорівнює 1100 лм. Це означає, що оптимальна кількість світильників у приміщенні дорівнює розрахунковій.

Наступним кроком підставимо всі відомі значення до формули (6.1) й дізнаємося загальне освітлення кабінету програмування:

$$E_p = \frac{1100 \times 18 \times 0,51}{35 \times 1,3 \times 1,1} = 201,8 \text{ (лк)} .$$

У ДБН В.2.5-28-2018 вказано, що рівень освітленості в приміщенні не повинен бути нижчим за 200 лк, тому можна зробити висновок, що рівень штучного освітлення у кабінеті програмування є достатнім.

Обладнання, які можуть створювати шум, знаходяться в досліджуваному приміщенні. Матричні принтери змінені на лазерні, що характеризуються значно низьким рівнем шуму. Тому при роботі принтера, ПК, кондиціонера, мобільного пристрою значення рівня шуму не перевищує 50 дБА. А такий результат відповідає санітарним нормам ДСН 3.3.6.037-99 .

У кабінеті постійно підтримується належний мікроклімат. В ній встановлені витяжна система, кондиціонери (механічна вентиляція) і природна вентиляція, яка відбувається при відкритті вікон. Температура повітря в приміщенні взимку складає 23-24°C, влітку коливається від 24°C до 25°C, відносна вологість повітря в приміщенні у теплий період складає біля 45%, а в холодний період становить 50%, швидкість руху повітря в холодний період спостерігається близько 0,1м/с, а в теплий період складає 0,2 м/с. Такі дані відповідають нормам, вказаних у ДСН 3.3.6.042-99[30].

Робота за комп'ютером супроводжується таким явищем, як випромінювання від моніторів. Згідно ДСНіП 3.3.6.096-2002 задля безпеки в кабінеті передбачено використання захисних екранів, а також проводиться контроль аеронізації повітря [31]. Під час безперервної роботи за ПК кожні 2 години працівник зобов'язаний дотримуватися 15-хвилинної перерви.

Робітники практично весь робочий час проводять сидячи, фізична активність мінімальна, інтенсивність енерговитрат до 120 ккал /год (до 139 Вт), відповідно категорія фізичних робіт - Іа. Згідно з ДСН 3.3.6.042-99 величини показників оптимальні для мікроклімату на робочих місцях.

Розглянувши наведений матеріал, можна зробити висновки про те, що умови праці відповідають всім нормам законодавства про охорону праці згідно зі законодавством України.

6.4 Заходи безпеки у надзвичайних ситуаціях

6.4.1 Заходи з пожежної безпеки

Пожежна безпека у виробничому приміщенні повинна забезпечуватися системою пожежного захисту та системою попередження пожежі, відповідно ДБН В 1.1.7-2002 «Захист від пожежі. Пожежна безпека об'єктів будівництва». Існує ряд факторів, що впливають на працівників та можуть призвести до виникнення пожежі, серед них підвищена температура повітря та предметів, знижена концентрація кисню, наявність токсичних продуктів згорання чи ушкодження споруд.

Для того, щоб забезпечити захист робочого приміщення від виникнення пожеж, слід використовувати максимальну кількість матеріалів та речовин, які важко спалахують, а також спеціальних меблів для робочого місця, покриттів для підлоги з негорючих матеріалів, встановити додаткові вогнеперегороджуючі пристрої, та забезпечити наявність у виробничому

приміщенні пристрою аварійного вимкнення та перемикання комунікацій та апаратів.

В приміщенні повинно бути об'ємно-планувальне виконання, в якому евакуація робітників повинна бути чітко спланована, та закінчуватися до початку обмежено допустимих рівнів опарних факторів пожежі, що встановлені санітарними нормами. Система вентиляції приміщення має бути обладнана пристроєм, що забезпечує автоматичне відключення вентиляції, в разі виникнення пожежі, а у вентиляційних каналах встановлені спеціальні пристрої, що затримують вогонь. Засоби сигналізації в приміщенні мають бути налаштовані таким чином, щоб оповіщення працівників розпочиналося з початкової стадії пожежі.

Для ліквідації пожежі на початковій стадії її виникнення, використовують такі первинні засоби пожежогасіння, як вогнегасники, системи автоматичного пожежогасіння, пожежний інвентар – ящики з піском, пожежні відра, пожежні стовбури, внутрішні пожежні водопроводи, покривала з негорючого теплоізоляційного полотна, азбестові ковдри і т.п. У приміщеннях пожежні крани встановлені в коридорах, на майданчиках сходових клітин та входів.

Комплектування технологічного устаткування вогнегасниками здійснено згідно з вимогами технічних умов (паспортів) на це устаткування або відповідними правилами пожежної безпеки. Вибір типу і розрахунок необхідної кількості вогнегасників в кабінеті, що досліджується, виконано в залежності від їх вогнегасної здатності, граничної площі, а також класу пожежі горючих речовин і матеріалів. З огляду того, що в кабінеті програмування знаходяться ПК, то у відповідності з законодавством передбачено наявність в кабінеті вогнегасників різних видів. Засобами гасіння вогнища загоряння в розглянутому приміщенні представлені вогнегасники ВП-5 та ВВ-3. Оскільки площа кабінету становить до 50 м², то достатньо двох п'яти кілограмових переносних порошкових вогнегасників ВП-5 та одного вуглекислотного вогнегасника ВВ-3. Вони розміщені в легкодоступних і помітних місцях на

висоті 1,2 м поблизу комп'ютерної техніки. Усе відповідає нормативу «Правила експлуатації та типові норми належності вогнегасників».

В залежності від матеріалу та речовини, відповідно ДБН В.1.1.7-2002 “Пожежна безпека об'єктів будівництва”, існує п'ять класів пожеж. Приміщення, де проводиться аналіз забезпечення безпеки ІС на основі капсульного методу належить до класів А та Е, оскільки воно має електроустановки під напругою (персональні комп'ютери) та меблі й канцелярське приладдя з речовин органічного походження, що супроводжуються тлінням.

Згідно НАПБ Б.03.002-2007 “Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою”, виробниче приміщення відноситься до категорії Д, через наявність прокладених кабельних електромереж, тому воно не характеризується як вибухонебезпечне чи пожежонебезпечне, але для додаткового захисту працівників в ньому встановлено ультразвуковий сповіщувач ДУЗ-4, що реагує на зміни характеристик ультразвукового поля.

Оскільки, у виробничому приміщенні наявний пристрій аварійного вимкнення та перемикач комунікацій та апаратів, а також система автоматичного пожежогасіння, нормовану кількість вогнегасників можна зменшити вдвічі – на кожні 20 м² площі встановлено один вуглекислотний вогнегасник.

6.4.2 Заходи з цивільного захисту

Біологічно небезпечні речовини і процеси, які характеризуються біологічною чи іншою дією або впливом, перевищують нормативні показники і загрожують життю або здоров'ю людини, є складовою частиною небезпечного явища, який являє собою небезпечний чинник.

У разі виникнення надзвичайних ситуацій центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері цивільного захисту, в межах своїх повноважень забезпечує реалізацію

державної політики в галузі медико-біологічного захисту населення. У повноваження органів місцевого самоврядування у сфері цивільного захисту входить також організація робіт по ліквідації наслідків надзвичайних ситуацій на відповідних територіях міст, муніципальних утворень і сіл, а також радіаційного, хімічного, біологічного, медичного та інженерного захисту територій від наслідків таких ситуацій.

До основних завдань цивільного захисту також відноситься усунення аварійних наслідків в умовах екстремальних температур, диму, газів, загрози вибухів, обвалів, зсувів, повеней, радіоактивного забруднення, хімічного і біологічного забруднення або іншого забруднення.

Стаття 37 Кодексу цивільного захисту України описує біологічний захист населення, тварин і рослин, що включає:

- 1) своєчасне виявлення факторів і вогнищ біологічної інфекції, їх локалізація і усунення;
- 2) прогнозування масштабів і наслідків біологічного зараження, розробка та виконання своєчасних протиепідемічних, профілактичних, протиепізоотичних, протиепіфітотичних і лікувальних заходів;
- 3) проведення неспецифічної і специфічної аварійної профілактики біологічного зараження населення;
- 4) своєчасне використання засобів індивідуального та колективного захисту;
- 5) введення обмежувальних протиепідемічних заходів, обсервації і карантину;
- 6) проведення дезінфекційних заходів в інфекційному вогнищі, дезінфекція господарюючих суб'єктів, тварин і санітарія населення;
- 7) надавати екстрену медичну допомогу людям, ураженим біологічними патогенами;
- 8) інші заходи біологічного захисту залежно від поточної ситуації[32].

Біологічний захист населення, тварин і рослин додатково включає встановлення протиепідемічного, протиепізоотичного та протиепіфітотичного

режимів і їх дотримання господарюючими суб'єктами, закладами охорони здоров'я та населенням.

Здійснення заходів біологічного захисту покладено на суб'єктів цивільного захисту.

З метою запобігання надзвичайним ситуаціям застосовується державне регулювання діяльності господарюючих суб'єктів в питаннях боротьби з лихами, включаючи моніторинг і прогнозування надзвичайних ситуацій. Щоб забезпечити виконання заходів щодо запобігання надзвичайним ситуаціям в Україні, надзвичайні ситуації постійно відстежуються і прогнозуються.

Моніторинг надзвичайних ситуацій - це система постійного спостереження, лабораторного та іншого контролю для оцінки стану захисту населення і територій, а також небезпечних процесів, які можуть призвести до загроз або надзвичайних ситуацій, і своєчасного виявлення тенденцій до їх зміни.

Спостереження, лабораторні та інші заходи контролю включають збір, обробку та передачу інформації про стан навколишнього середовища, забруднення харчових продуктів, продовольчої сировини, кормів, води радіоактивними і хімічними речовинами, зараження інфекційними захворюваннями та іншими небезпечними біологічними агентами.

ВИСНОВКИ

У ході виконання магістерської роботи були розглянуті наступні питання, як: дослідження існуючих видів і методів захисту ІС від НСД, різновиди ідентифікації, автентифікації, управління доступом з застосуванням технічних засобів.

Проведений аналіз методів ШНМ для захисту від НСД, їх архітектури та особливостей застосування в практичних задачах кібербезпеки дозволяє зробити висновок, що метод капсульних нейронних мереж - вкрай перспективна архітектура штучних нейромереж для вирішення задач захисту ІС від НСД, таких як: розпізнавання об'єктів на зображеннях та відео, розпізнавання тексту та використання у ОПМ, розпізнавання кіберзагроз та класифікація типів шкідливого ПЗ. Був описаний процес навчання капсульних нейронних мереж, який здійснюється за допомогою динамічної маршрутизації між капсулами. Капсульні мережі знижують помилку розпізнавання об'єкта в іншому ракурсі в порівнянні зі ЗНМ. В даний час дана архітектура модифікується і допрацьовується з метою отримання результатів на порівняно меншому обсязі даних, ніж цього вимагають ЗНМ.

У даному проєкті була розроблена методика використання капсульного методу для задач забезпечення захисту ІС від НСД. Таким чином, було запропоновано впроваджувати КНМ у системи розпізнавання облич на фото та відео, що може використовуватися для ідентифікації та автентифікації. Також, даний метод може використовуватися у виявленні презентаційних атак в біометричних системах автентифікації і задля виявлення людських дій на відео. Дана методика також пропонує використовувати капсульний метод для аналізу тексту та обробки природної мови для розпізнавання кіберзагроз на прикладі соціальної мережі Twitter. Капсульний метод може бути впроваджено у класифікацію шкідливих програм. При розробці даної методики були проаналізовані можливі напрями розвитку капсульного методу для

використання у захисті ІС від НСД, такі як розпізнавання та класифікація трафіку мережі, у виявленні ботнетів і генерації шкідливих доменних імен, при виявленні і зменшенні шкоди атак завантаження, а також для виявлення вторгнень в ІС.

Матеріал, що був викладений у даній магістерській роботі пройшов апробацію та опублікован у [33].

Також, у даному проєкті були визначені маркетингові аспекти, а саме: описана ідея проєкту, проведена попередня характеристика потенційного ринку та клієнтів, зроблений SWOT-аналіз, обрані групи потенційної цільової аудиторії, а також складена карта стейкхолдерів. Також, була розрахована собівартість на 90 днів реалізації проєкту, що складає 218591,35 грн. з урахуванням заробітної плати молодшого наукового співробітника, його керівника і лаборанта, та їх ЄСВ. Також, були розраховані вартість спожитих послуг, в тому числі і специфічного обладнання, а також – амортизація до нього за 3 місяці. Була розрахована економія від аналізу капсульного методу нейромереж для забезпечення безпеки ІС від НСД, яка складає 50208,65 грн.

Було досліджено аспекти охорони праці та безпеки при надзвичайних ситуаціях, проведений розрахунок рівня освітлення приміщення, зроблено аналіз потенційних небезпек, розглянуті заходи по забезпеченню безпеки, виробничої санітарії та гігієни праці, пожежної безпеки, які демонструють, що дане приміщення відповідає усім санітарним нормам та правилам. Також розглянуті заходи з цивільного захисту, у яких описаний біологічний захист населення.

Результати даної роботи можуть бути використані власниками ІС та спеціалістами з кібербезпеки для удосконалення існуючих систем захисту від НСД. Розроблена методика дозволяє обширно подивитись на використання капсульного методу при впровадженні різних систем безпеки, починаючи з ідентифікації користувача, і закінчуючи аналізом мережного трафіка. Дана методика може дуже стрімко вивести системи захисту на більш високий рівень, при тому, що КНМ як і інші нейромережі можуть самовдосконалюватися

шляхом навчання у процесі роботи, що зробить системи, у яких вони впроваджені, більш швидкодіючими та автоматизованими.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Нестеров, С.А. Информационная безопасность и защита информации: навч. посіб. / С.А. Нестеров - СПб. : Издательство Политехнического университета, 2009. - 126 с.
2. Про захист інформації в інформаційно-телекомунікаційних системах : [закон України : від 05.07.1994 № 80/94-ВР] // Відомості Верховної Ради України. - 1994. - № 31. - с. 286.
3. Захист інформації від несанкціонованого доступу / Бібліофонд - Режим доступу: URL :<https://www.bibliofond.ru/VIEW.ASPX?ID=721960/> - 23.02.2014 р
4. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : [Постанова, Правила України : від 29 березня 2006 р. N 373-ВР] // Кабінет Міністрів України. – 2006. – 373. – с.164.
5. Козачок, В.А. Особливості ідентифікації та авторизації в сучасних корпоративних інформаційно-телекомунікаційних системах / В.А. Козачок, М.В. Діхтяр, О.В. Семко // Сучасний захист інформації. – 2017. - №2(30), С. 42-48.
6. Штучна нейронна мережа / Вікіпедія. - Режим доступу: URL : https://ru.wikipedia.org/wiki/Искусственная_нейронная_сеть/ - 15.05.2018 р.
7. Хайкін, С. Нейронні мережі: повний курс, 2-е видання. / С. Хайкін; пер з англ. Н . Куссуль . - М . : Видавничий дім «Вільямс» , 2006 , - 1104 с.
8. Свёрточная нейронная сеть / Вікіпедія. - Режим доступу: [www . URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D1%91%D1%80%D1%82%D0%BE%D1%87%D0%BD%D0%B0%D1%8F_%D0%BD%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C/](https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D1%91%D1%80%D1%82%D0%BE%D1%87%D0%BD%D0%B0%D1%8F_%D0%BD%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C/) - 22.04.2020 р.

9. Mukhometzianov, R. CapsNet comparative performance evaluation for image classification / R. Mukhometzianov, J. Carrillo. – Canada: University of Waterloo, 2018. – 14 p. – Режим доступа: URL : <https://arxiv.org/ftp/arxiv/papers/1805/1805.11195.pdf>. – 22.03.2019.
10. Xi, Ed. Capsule Network Performance on Complex Data / Ed. Xi, S. Bing, Y. Jin. – Pittsburgh: Carnegie Mellon University, 2017. – 7 p. – Режим доступа: www . URL : <https://arxiv.org/pdf/1712.03480.pdf>. – 22.03.2019.
11. Hinton, G. E. Dynamic Routing Between Capsules / S. Sabour, N. Frosst, G. E. Hinton. – Toronto: Google Brain, 2017. – Режим доступа: www . URL : <https://arxiv.org/pdf/1710.09829.pdf>. – 22.03.2019.
12. Hinton, G. E. Matrix capsules with EM routing / G. E. Hinton, S. Sabour, N. Frosst. – Toronto: Google Brain, 2018. – 15 p. – Режим доступа: www . URL : <https://openreview.net/pdf?id=HJWLfGWRb>. – 22.03.2019.
13. Lin, A. On Learning and Learned Representation with Dynamic Routing in Capsule Networks / A. Lin, J. Li, Z. Ma. – Guangdong: Guangdong Polytechnic Normal University, 2018. – 12 p. – Режим доступа: <https://arxiv.org/pdf/1810.04041.pdf>. – 22.03.2019.
14. Pechyonkin, M. Understanding Hinton's Capsule Networks. Part IV: CapsNet Architecture / M. Pechyonkin, - Режим доступа: www . URL : <https://medium.com/ai%C2%B3-theory-practice-business/part-iv-capsnet-architecture-6a64422f7dce> - 21.02.2018 p.
15. Pechyonkin, M. Understanding Hinton's Capsule Networks. Part III: Dynamic Routing Between Capsules / M. Pechyonkin, - Режим доступа: www . URL : <https://medium.com/ai%C2%B3-theory-practice-business/understanding-hintons-capsule-networks-part-iii-dynamic-routing-between-capsules-349f6d30418> - 29.11.2017 p.
16. ISO/IEC 30107-1:2016. Information technology — Biometric presentation attack detection [Электронный ресурс]. — Режим доступа: <https://www.iso.org/standard/53227.html> - 01.01.2016

17. Nguyen, H. Use of a capsule network to detect fake images and videos / H. Nguyen, J. Yamagishi, I. Echizen. - ArXiv abs/1910.12467 (2019) - [Електронний ресурс]. — Режим доступу: <https://arxiv.org/pdf/1910.12467v2.pdf> - 29.10.2019.
18. Duarte K. VideoCapsuleNet: A Simplified Network for Action Detection / K. Duarte, Y. Rawat, M. Shah. - arXiv:1805.08162v1 - [Електронний ресурс]. — Режим доступу: <https://arxiv.org/abs/1805.08162> - 21.05.2018.
19. Обробка природної мови / Вікіпедія. - [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Обробка_природної_мови - 17.10.2020.
20. Liqiang X. MCapsNet: Capsule Network for Text with Multi-Task Learning / X. Liqiang, H. Zhang, W. Chen, Y. Wang, Y. Jin. – Association for Computational Linguistics, Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing. - [Електронний ресурс]. — Режим доступу: <https://www.aclweb.org/anthology/D18-1486> - 31.10.2018.
21. Altalhi1 S. Capsule Network for Cyberthreat Detection / S. Altalhi, M. Abulkhair, E. Alkayal - International Journal of Advanced Computer Science and Applications (IJACSA). - [Електронний ресурс]. — Режим доступу: <http://dx.doi.org/10.14569/IJACSA.2020.0110673> - 06.11.2020.
22. Cayir A. Random CapsNet Forest Model for Imbalanced Malware Type Classification Task / A. Cayir, U. Unal, H. Dag - eprint arXiv:1912.10836. - [Електронний ресурс]. — Режим доступу: https://ui.adsabs.harvard.edu/link_gateway/2019arXiv191210836C/arxiv:1912.10836 – 20.12.2019.
23. Berman, D. S. A Survey of Deep Learning Methods for Cyber Security / D. S. Berman, A. L. Buczak, J. S. Chavis, C. L. Corbett - Information. – 2019. – Т. 10. – №. 4. – С. 122. - [Електронний ресурс]. — Режим доступу: <https://www.mdpi.com/2078-2489/10/4/122> - 14.01.2019 р.
24. Класифікація інвестицій [Електронний ресурс]. – Режим доступу: https://studme.com.ua/1314021610664/finansy/klassifikatsiya_investitsiy.htm

25. НПАОП 40.1-1.21-98. Правила безпечної експлуатації електроустановок споживачів [Електронний ресурс]. — Режим доступу: https://dnaop.com/html/2029/doc-НПАОП_40.1-1.21-98

26. НПАОП 0.00–4.12.05. Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці [Електронний ресурс]. — Режим доступу: https://dnaop.com/html/32368/doc-НПАОП_0.00–4.12.05

27. ДСТУ ISO 7010:2009. Графічні символи. Кольори та знаки безпеки. Знаки безпеки, використовувані на робочих місцях і в місцях громадської призначеності [Електронний ресурс]. — Режим доступу: <https://metrology.com.ua/ntd/skachat-iso-iec-ohsas/iso/dstu-is0-7010-2009/>

28. ДСанПиН 3.3.2-007-98. Гигиенические требования к организации работы с визуальными дисплейными терминалами электронно-вычислительных машин [Електронний ресурс]. — Режим доступу: https://dnaop.com/html/40949/doc-ДСанПиН_3.3.2-007-98

29. ДБН В.2.5-28:2018 Природне і штучне освітлення [Електронний ресурс]. — Режим доступу: https://dbn.co.ua/load/normativy/dbn/dbn_v_2_5_28/1-1-0-1188

30. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень освітлення [Електронний ресурс]. — Режим доступу: http://online.budstandart.com/ru/catalog/doc-page?id_doc=14283

31. ДСанПиН 3.3.6.096-2002 Государственные санитарные нормы и правила при работе с источниками электромагнитных полей освітлення [Електронний ресурс]. — Режим доступу: http://online.budstandart.com/ru/catalog/doc-page.html?id_doc=48146

32. Кодекс цивільного захисту України [Текст] : [прийнятий ВР України 02.10.2012 р. № 5403-VI] : офіц. текст : станом на 06.12.2012 р. / ВР України. — К. : Алерта, 2012. — 120 с. ; 20 см. — 3000 прим. — ISBN 978-617-566-172-7.

33. Матвейчук, О.В. Використання методів штучних нейронних мереж для захисту комп'ютерів від несанкціонованого доступу / О.В. Матвейчук, В.О.

Воскобойник // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених, аспірантів та студентів, 13-17 квітня 2020 р.: тези доповідей. – Запоріжжя, 2020. – с. 91-93.