МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ЕЛЕКТРОНІКИ, РОБОТОТЕХНІКИ І ТЕХНОЛОГІЙ МОНІТОРИНГУ
ТА ІНТЕРНЕТУ РЕЧЕЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Шутко В.М.
«____»_____ 2020 р.

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА
ЗІ СПЕЦІАЛЬНОСТІ 153 «МІКРО- ТА НАНОСИСТЕМНА ТЕХНІКА»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ФІЗИЧНА ТА БІОМЕДИЧНА ЕЛЕКТРОНІКА»

Тема: «Системи доступу до приміщень з використанням штучного інтелекту»

Виконавець
студент групи МН-206м _____ Довженко Р. В.

Керівник
д.т.н., професор _____ Ліпінський О.Ю.

Консультант розділу
«Охорона праці» _____ Якимець І.В

Консультант розділу
«Охорона навколишнього середовища» _____ Мадж С.М.

Нормоконтролер _____ Сініцин Р.Б.

КИЇВ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет аеронавігації, електроніки та телекомунікацій
Кафедра електроніки, робототехніки і технологій моніторингу та інтернету речей
Освітньо-кваліфікаційний рівень Магістр
Напрям (спеціальність) 153 «МІКРО- ТА НАНОСИСТЕМНА ТЕХНІКА»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ФІЗИЧНА ТА БІОМЕДИЧНА ЕЛЕКТРОНІКА»»

ЗАТВЕРДЖУЮ
Завідувач випускової кафедри
_____Шутко В.М.
«____»_____ 2020 р.

ЗАВДАННЯ
на виконання дипломного проекту (роботи) студента
Довженко Руслан Вадимович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи): «Системи доступу до приміщень з використанням штучного інтелекту» затверджена наказом ректора від «02» жовтня 2020 р. № 1900 / ст
2.Термін виконання проекту (роботи): 05.10.2020 по 27.12.2020
3.Вихідні дані:Статистичні та аналітичні дані на основі систем безпеки.
4.Зміст пояснювальної записки (перелік питань, що підлягають обробці):аналіз методів контролю доступу, огляд систем контролю доступу, огляд методів інтелектуального аналізу даних, огляд методів машинного навчання та програмного забезпечення, розробка архітектури, розробка алгоритмічного забезпечення.
5.Перелік обов'язкового графічного матеріалу: таблиці, рисунки, графіки.
6.Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Ознайомлення з тематикою дипломної роботи.		
2.	Обробка матеріалів за темою дипломної роботи.		
3.	Розробка алгоритмічного забезпечення.		
4.	Розробка програмного забезпечення.		
5.	Написання вступу та висновків.		
6.	Оформлення пояснювальної записки та пре-		

	зентації.		

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	К.т.н., доцент Якимець І.В.		
Охорона навколишнього середовища	К.б.н., доцент Мадж С.М.		

8.Дата видачі завдання: “_____”_____ 2020 р.

Керівник дипломної роботи (проекту) _____ Ліпінський О.Ю.

(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Довженко Р.В

(підпис випускника) (П.І.Б.)

ЗМІСТ

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Системи доступу до приміщень з використанням штучного інтелекту» містить: 72 сторінки, 19 рисунків, 24 використаних джерел.

БЕЗПЕКА, СИСТЕМА ДОСТУПУ, ШТУЧНИЙ ІНТЕЛЕКТ, НЕЙРОННІ МЕРЕЖІ.

Об’єкт дослідження – приміщення. Предмет дослідження – система доступу до приміщення.

Мета дипломної роботі – розробити архітектуру та алгоритмічне забезпечення для контролю доступу до приміщень та реалізувати механізм виявлення загрози.

Новизна – удосконалення процесу контролю доступу до приміщень, шляхом розроблення методів та алгоритмічного забезпечення, що грунтується на аналізі даних з наявних систем контролю доступу із застосуванням методів штучного інтелекту для реалізації механізму виявлення загроз та небезпечних ситуацій.

ВСТУП

Для компаній або приватних осіб зі складними вимогами до захисту, вагому частину операцій по забезпеченню безпеки являє людська робоча сила. Проте, підвищений попит на персонал моніторингу, а також охоронців в поєднанні з нестачею робочої сили, призводить до вагомого перевантаження ресурсів безпеки цих компаній. При розгляді проблем забезпечення безпеки життя, підвищення фізичної безпеки і підвищення відповідальності співробітників і підрядників з'являється більше можливостей, ніж будь-коли раніше. Важливо розробити всеосяжний план, що включає рівні захисту і використовує відповідні технології для допомоги, а не заміни людей, відповідальних за фізичну безпеку. Це робить інтелектуальні технології дуже необхідними.

В останні роки одними з найпопулярніших інтелектуальних апаратних продуктів є інтелектуальні дверні замки. Відповідні дані показують, що в 2016 році глобальна індустрія інтелектуальних дверних замків досягла 11 мільйонів комплектів, з яких 1,5 мільйона комплектів знаходяться в Японії, 1,7 мільйона – в Південній Кореї, 2,5 мільйона – в Європі і США, 3,5 мільйона – в Китаї і 2 мільйони на інших ринках світу. До 2021 року світова промисловість досягне 51 млн. комплектів, середньорічні темпи зростання яких складуть близько 40%.

Хоча турнікети, можливо, не зазнали кардинальних змін за формою, їх використання в багаторівневому рішенні безпеки може надати безцінні дані для вирішення на основі штучного інтелекту. Аномальні схеми руху або незвичайний доступ можуть бути виявлені до того, як люди досягнуть зон підвищеної безпеки. Рандомізовані вибіркові перевірки, контрольована пропускна здатність і спрямовані потоки трафіку можуть ініціюватися і управлятися за допомогою інтелектуальних рішень, заснованих на оцінці ризиків, у міру виявлення загроз.

Ніякі пристрої фізичної безпеки не отримали більшої вигоди від штучного інтелекту, ніж системи контролю фізичного доступу. При інтеграції з рішенням на основі штучного інтелекту система контролю доступу тепер може швидко реагувати на

загрози і відповідним чином налаштовувати дозволи. Можливість виявляти аномальні події, внутрішні загрози та небезпечні ситуації і динамічно змінювати дозволи є великим проривом в світі фізичної безпеки.

Сценарії використання в цій категорії дуже різноманітні. Наприклад. Коли штучний інтелект застосовується для контролю доступу, він може ідентифікувати незвичайну активність, таку як доступ в неробочий час і ненормальний доступ до місця розташування, і поєднувати її з іншими індикаторами загроз для швидкого виявлення внутрішніх загроз. Доступ з адаптацією до ризику може запобігти потраплянню людей в зону, де знаходиться традиційно «неочевидна» небезпека, і він може дозволити особам, послугами якої є перша допомогу, з відповідними обліковими даними, отримати доступ в зону, в іншому випадку обмежену, коли існують загрозливі умови.

В галузевому звіті Security Information Watch мовиться: «Завдяки досягненням в мобільних технологіях, хмарних технологіях, штучному інтелекті, біометрії на мобільних і переносних пристроях контроль доступу тепер більш інтегрований з тим, що вважається «сучасним».

РОЗДІЛ 1 Аналіз методів контролю доступу

1.1. Контроль доступу

Контроль доступу визначається як процес вибіркового обмеження й управління можливістю входу або виходу з певної області. Системи контролю доступу призначені для забезпечення доступу уповноважених осіб в будівлю, кімнату або іншу зону з обмеженням доступу неуповноважених осіб. Для підприємств запобігання несанкціонованого доступу має важливе значення для мінімізації ризику.

Обрана система контролю доступу повинна бути функціональною, оскільки вона буде відігравати важливу роль в повсякденних операціях. Комерційні системи контролю доступу можуть відрізнятися за складністю та володіти великою кількістю функцій. Ефективна система забезпечує швидкий і зручний доступ для уповноважених осіб, надійно обмежуючи при цьому інших.

Системи контролю доступу розвивалися протягом багатьох років у міру зростання потреб в безпеці бізнесу. Замість того, щоб покладатися на механічні ключі, охоронців і паперові листи для входу в систему, електронні системи контролю доступу використовують комп'ютери та передові технології для поліпшення контролю і моніторингу.

Існує два різні стилі систем контролю доступу: мережеві (IP) системи і традиційні автономні системи. Також існує три основних способи управління дозволами на доступ для цих систем. Тип системи, який найкраще підходить для конкретного завдання, залежить від наявної безпеки і потреб [1].

1.1.1. Обов'язковий контроль доступу (ОКД)

Обов'язковий контроль доступу зазвичай вважається найбільш суворим типом контролю доступу. Всі двері контролюються налаштуваннями, створеними системними адміністраторами. У цій системі користувачі не можуть змінювати дозволи, які забороняють або дозволяють їм вхід в різні кімнати на об'єкті, тим самим забезпечуючи безпеку конфіденційних документів і даних [1]. Система також обмежує

можливість власника області або ресурсу забороняти або надавати доступ до ресурсів, перерахованих в файлової системі. Всі кінцеві користувачі класифіковані і забезпечені мітками, які дозволяють їм отримати доступ тільки відповідно до встановлених правил безпеки. Наприклад, рівень доступу користувачів і класифікація даних (як конфіденційні, секретні або цілком таємні) використовуються в якості міток безпеки для визначення рівня довіри. ОКД обмежує доступ до ресурсів в залежності від ступеня конфіденційності інформації, що міститься в ресурсі, і дозволу користувача на доступ до інформації з таким рівнем конфіденційності. Він зазвичай використовується державними установами та військовими, оскільки в ньому робиться наголос на послідовну класифікацію і конфіденційність даних. ОКД часто розглядається як протилежність наступного типу управління контролем доступу, дискреційного контролю доступу.

1.1.2. Дискреційний контроль доступу (ДКД)

Дискреційний контроль доступу дозволяє власникам бізнесу вирішувати, хто може отримати доступ до яких областей приміщення або ресурсів. Власник даних має повний контроль над усіма програмами і файлами в своїй системі і визначає, хто може отримати доступ до певних ресурсів [1]. Тому вони несуть відповідальність за визначення людей, які можуть увійти в певне місце, цифровим або фізичним способом. Наприклад, системний адміністратор може створити ієрархію файлів для доступу на основі певних дозволів. Аутентифікація користувача заснована на наданих облікових даних, таких як ім'я користувача і пароль. Потім цей тип управління доступом пропонує вибіркове обмеження, гарантуючи, що користувачі, які звертаються до системи, мають дозвіл на перегляд даних компанії.

ДКД простий в реалізації та інтуїтивно зрозумілий, але може бути не найкращою системою через деяких своїх недоліків. Одним з недоліків є те, що кінцевий користувач має повний контроль над налаштуванням рівня безпеки для інших користувачів, що обмежує контроль авторизації. Крім того, ця система вимагає більш активного управління для відкликання і надання дозволів, ніж жорстка система.

ДКД часто розглядається як протилежність його більш структурованого і жорсткого аналогу ОКД.

1.1.3. Контроль доступу на основі ролей (КДОР)

Контроль доступу на основі ролей призначений для дозволу або обмеження доступу на основі певних ролей з викладеними бізнес-обов'язками, а не для окремого користувача. Роль співробітника в організації визначає дозволи, які йому надаються, і гарантує, що співробітники нижнього рівня не може отримати доступ до конфіденційної інформації або виконувати завдання високого рівня [1]. КДОР - це найбільш поширена форма управління дозволами користувачів. Цей метод розроблений з використанням прав доступу, заснованих на змінних атрибутах, таких як потреби в ресурсах, завдання, середа, місце розташування і т. д.

Це спрощує власникам можливість управляти користувачами в групах в залежності від їх ролі або положення, а не призначати дозволи кожної конкретної людини. КДОР в значній мірі виключає свободу дій при наданні доступу до об'єктів. Наприклад, фахівець з персоналу не повинен мати дозволів на створення мережевих облікових записів; ця роль повинна бути зарезервована для мережевих адміністраторів. Компанії в значній мірі покладаються на цю модель для захисту своїх конфіденційних даних і критично важливих додатків. Підвищення ефективності роботи, підвищення відповідності нормативним вимогам, підвищення прозорості для адміністраторів, зниження витрат і зниження ризику витоків і витоку даних. Безпека на основі ролей - це гнучкий і безпечний метод управління дозволами користувачів.

1.1.4. Контроль доступу на основі правил (КДОП)

У цьому типі управління системою права доступу засновані на структурованих правилах і політиках. Цей метод в значній мірі заснований на контексті з наданням або відмовою в доступі на основі набору правил, визначених системним адміністратором. Коли обліковий запис або група намагається отримати доступ до ресурсу, операційна система перевіряє правила, що містяться в списку управління доступом для цього об'єкта [1].

Хоча доступ до управління на основі правил простий для розуміння, його часто комбінують з контролем доступу на основі ролей, щоб краще застосовувати процедури та політики. Наприклад, класифікуючи роль і правила, адміністратори можуть встановлювати дозволу, що дозволяють студентам відвідувати лабораторію в певний час дня.

1.1.5. Контроль доступу до атрибутів (КДА)

Цей тип управління також відомий як контроль на основі політик, оскільки він забезпечує різний динамічний та інтелектуальний контроль на основі певних атрибутів користувача [1]. Атрибути використовуються як будівельні блоки, які описують запити доступу і визначають управління доступом. Потім встановлені політики можуть використовувати будь-який з цих атрибутів: атрибути об'єкта, атрибути ресурсу, атрибути середовища або користувача, щоб визначити, чи повинен користувач мати доступ.

Незважаючи на те, що КДА заснований на рольовому управлінні доступом, це просунутий спосіб визначення доступу з використанням таких атрибутів, як група, відділ, статус співробітника, громадянство, посаду, тип пристрою, IP-адреса або будь-які інші фактори. Ці атрибути також можна отримати і імпортувати з бази даних, сервера або навіть від ділового партнера, що допомагає йому працювати з більшими бізнес-функціями.

1.1.6. Контроль доступу на основі ідентифікації (КДОІ)

КДОІ – це спрощений метод безпеки, який визначає, дозволено або заборонено особі використовувати даний електронний ресурс на основі їх індивідуальної візуальної ідентичності [1]. Отже, користувачеві буде дозволений або заборонений доступ до електронного ресурсу в залежності від того, чи може його особистість збігатися з ім'ям, яке з'являється в списку управління доступом. Використовуючи це, мережеві адміністратори можуть більш ефективно управляти діями і доступом в залежності від індивідуальних потреб. Деякі з переваг підходу до безпеки, заснованого на ідентифікаційних даних, включають здатність здійснювати дуже детальний конт-

роль над тим, які служби і які функції активно виконують ці люди. Крім того, є перевага, що полягає в можливості застосовувати політику контролю доступу на різних пристроях, таких як смартфони, планшети і ПК.

1.1.7. Контроль доступу на основі історії (КДОІС)

Рішення, що приймаються цією системою управління доступом, в основному ґрунтуються на минулих діях щодо забезпечення безпеки [1]. Історичні події користувача визначають, чи буде йому надано доступ. Це вимагає оцінки історії дій користувача в реальному часі, такий як час між запитами, зміст запитів, які двері були недавно відкриті і т.д. Як приклад можна надати доступ до певної службі або джерела даних або відхилено через минуле поведінки користувача, наприклад, інтервал запиту перевищує один запит в секунду.

1.1.8. Організаційний контроль доступу (ОРКД)

ОРКД допомагає при оцінці політик безпеки і дозволів більших організацій з декількома користувачами, наприклад сторонніх компаній [1]. Цей метод забезпечує високу ступінь масштабованості та виразності. Кожна політика безпеки визначається організацією і для неї всередині більшої системи. Таким чином, специфікація політики безпеки повністю параметрізуется організацією, тому можна одночасно обробляти кілька політик безпеки, пов'язаних з різними організаціями.

1.1.9. Відповідальний контроль доступу (ВКД)

Системи, засновані на відповідальності, обмежують вхід або доступ відповідно до їхніх обов'язків в організації [1]. Працівники можуть отримати доступ лише до інформації, яка необхідна їм для виконання своїх службових обов'язків. Такі фактори, як відповідальність, посадова компетентність та повноваження, використовуються для визначення того, хто відповідальний, щоб мати доступ до певної інформації. Це гарантує, що працівники низького рівня не отримуватимуть доступ до конфіденційних даних бізнесу, які можуть бути використані проти компанії.

1.2. Можливості для різних типів систем контролю доступу

1.2.1. Хмарне керування доступом (ХКД)

Це найкраще рішення для забезпечення безпеки вашого об'єкта, що забезпечує набагато більш високий рівень безпеки, необмежену масштабованість, мінімальні зусилля, більшу зручність і простоту обслуговування [2]. Дозволи на доступ зберігаються, управляються і обробляються в мережі віддалених серверів, розміщених в Інтернеті, а не на локальних серверах або персональних комп'ютерах. Це дозволяє адміністратору керувати дозволами з будь-якого місця і в будь-який час, просто використовуючи браузер. На відміну від інших моделей контролю доступу, які споживають багато ресурсів, ХКД економить внутрішні ресурси і пропонує підписки, які можуть збільшити прибуток вашої компанії.

1.2.2. Локальний контроль доступу (ЛКД)

ЛКД пропонує рівень безпеки і контролю, який просто неможливий в хмарі. Бізнес може контролювати, управляти і обробляти дані своїм власним персоналом або IT-персоналом. Права доступу реалізуються на локальних серверах або персональних комп'ютерах, які щодня управляються внутрішньою службою безпеки, IT-персоналом або обома. Ці програмні платформи контролю доступу потребують регулярного обслуговування для забезпечення належного функціонування. Немає сумнівів в тому, що традиційний ЛКД зарекомендував себе як високоефективне рішення для забезпечення фізичної безпеки в усьому світі [2].

1.2.3. Системи контролю доступу на базі мобільних пристроїв або смартфонів (СКДМП)

Це використання мобільного пристрою, такого як смартфон, планшет або переносна пристрій, для отримання доступу до системи безпеки дверей, воріт, мереж, послуг і багато чого іншого [2-3]. Попит на Mobile-First зростає в усьому світі, що робить СКДМП найбільш важливим компонентом для захисту різних підприємств.

1.2.4. Системи контролю доступу на основі Інтернету речей (СКДІоТ)

Пристрої Інтернету речей відіграють вирішальну роль, допомагаючи організаціям конкурувати на сучасному цифровому ринку, тому Інтернет речей являє собою унікальний набір проблем контролю доступу через низький енергоспоживання пристроїв Інтернету речей, низької пропускної здатності між пристроями Інтернету речей та Інтернетом, розподіленого характеру системи, однорангові мережі і потенційна потреба в надзвичайно великій кількості пристроїв IoT [3]. Ця модель підключає всі дверні зчитувачі до Інтернету і має вбудоване ПЗ, яке можна оновлювати з міркувань безпеки або для додавання нових функцій. На високому рівні є два способи реалізувати контроль доступу для IoT:

Централізована архітектура – користувач отримує доступ тільки до хмарним серверів, які авторизують запити і передають дані між користувачем і пристроями IoT.

Розподілена архітектура – сервер управління доступом надає маркери доступу користувачам, які використовують їх для прямого доступу до пристроїв IoT.

1.3. Огляд систем контролю доступу

У цьому підрозділі подано огляди деяких найкращих систем на ринку на основі [4], а також подробиці функцій, які ці системи включають.

Назва компанії	Тип системи	Професійна установка	Ключові особливості
Kisi	На основі хмари	Так	Сумісний з iOS та Android, віддалене управління
ISONAS	Чистий IP	Немає	Мінімальне обладнання, двосторонній зв’язок із несанкціонованим доступом, надійне шифрування даних
Johnson Controls	Інтернет	Так	Планування блокування дверей, моніторинг сигналізації, управління дозволами

ADT	Електронний	Так	Обслуговування в той же день, моніторинг руху, інтеграція з іншими системами сигналізації
Vanderbilt Industries	На основі хмари	Так	Контрольоване блокування, легке масштабування, інтеграція з іншими програмами

1.3.1. Kisi

Параметри обладнання та програмного забезпечення Kisi дуже прості, пропонується два варіанти зчитувача та один контролер, що робить установку швидкою та простою [5].

Kisi пропонує інтеграцію з більш ніж 20 послугами, включаючи CRM, системи планування та управління даними. Kisi не пропонує інших аварійних варіантів, таких як пожежа, газ та аварійні сигнали. Kisi зосереджується на забезпеченні спрощеної сучасної системи, яка добре працює для будь-якого виду бізнесу. Завдяки широкому діапазону варіантів доступу співробітників, мобільному додатку для віддаленого управління та інтеграції з іншими службами ви можете створити лише налаштування контролю доступу, що відповідають вашим потребам у бізнесі [5].

Обладнання Kisi має наступні варіанти:

- Kisi Reader Pro за 599 доларів
- Kisi Reader Pro Outdoor за 699 доларів
- Kisi Controller Pro за 899 доларів

Програмне забезпечення поставляється в трьох варіантах плану, кожен з яких включає інформаційну панель управління Kisi та мобільні дані. Ліцензії встановлюються на кожного користувача та на двері щомісяця, щороку чи багато років. Вам потрібно буде зв’язатися з Kisi, щоб отримати персональну пропозицію щодо програмного забезпечення. Ось розбивка кожного плану:

Основні	Стандартний	Про

Один адміністратор 30 днів зберігання подій Стандартна підтримка	П'ять адміністраторів 120 днів зберігання подій Синхронізація користувача Веб-панель інструментів Стандартна підтримка	Необмежена кількість адміністраторів Аутентифікація користувача Необмежене зберігання та експорт подій Пріоритетна підтримка

Kisi також пропонує кілька варіантів доступу до будівлі. Працівники можуть використовувати телефони, ключові картки або брелоки, які працюють із пристроєм зчитування, для доступу до вашого закладу. Можна налаштувати систему на надання доступу за допомогою тимчасового посилання, надісланого на телефон працівника. Смартфони, що мають біометричні функції автентифікації, можуть використовуватися для автентифікації, щоб відкрити двері замість пароля. Процес автентифікації є власною та зашифрованою.

Система має інтерфейс звітування та адміністрування, який також доступний через мобільний пристрій. Він також може складати повні звіти про аудит, відстежувати двері в режимі реального часу та експортувати дані. Можна встановити сповіщення, які попереджатимуть, коли двері відчиняться у незвичний час.

Kisi може інтегруватися з більш ніж 20 послугами, включаючи планування, спостереження, дані та інше програмне забезпечення. Є можливість інтегрувати систему Kisi із типовими бізнес-додатками, такими як Okta, Verkada, Google Apps та Mindbody. Компанія також пропонує сигналізацію про вторгнення.

Система масштабована і легко охоплює кілька місць за допомогою централізованої системи віддаленого управління та каталогу, який синхронізується безпосередньо з вашими дверима, дозволяючи лише доступ затвердженим сторонам.

Kisi пропонує зразкову підтримку та варіанти ресурсів на своєму веб-сайті, включаючи опис систем контролю доступу та розділ спільноти, де ви знайдете різні відповіді та теми, що стосуються системи контролю доступу Kisi.

1.3.2. ISONAS

ISONAS легко встановити, з попередньо налаштованими зчитувачами та простою вимогою до мережевого підключення. Розумні читачі можуть приймати рішення щодо автентифікації та відкривати двері, навіть якщо мережа не працює. Це не комплексна система - немає аварійних сигналів про затримку чи пожежу [6].

ISONAS забезпечує Pure IP-контроль доступу, який використовує ваше існуюче підключення до мережі, а не залежно від проводки та панелей на кожних дверях. ISONAS також продає обладнання для перетворення старих систем на IP-системи, сумісні з набором програмного забезпечення для управління доступом.

ISONAS - це бюджетна система, оскільки вона вимагає порівняно небагато обладнання та відсутність програмної інфраструктури. Система також має просту установку та веб-навчання, що сприяє зниженню витрат.

ISONAS пропонує два варіанти програмного забезпечення [6]:

1. Хмара чистого доступу
    a. Повністю розміщена версія в хмарі
    b. Контролери зчитувача, попередньо налаштовані на хмару
    c. Легко вставати і працювати
    d. Менеджер чистого доступу
2. Локальна версія Pure Access
    a. Дозволяє керувати системою контролю доступу з будь-якого пристрою у вашій мережі

Для апаратного забезпечення знадобляться щонайменше зчитувач, контролер та облікові дані, будь то фізичні (наприклад, ключові картки та брелоки) або мобільні (як додаток).

Найбільша привабливість ISONAS полягає в тому, що пропонується мінімальне обладнання та просте у використанні програмне забезпечення із хмарною системою управління. Це дозволяє дуже малим підприємствам легко створити та забезпечити (і управляти) доступ для своїх працівників.

ISONAS пропонує варіанти доступу для зчитування дверей у двох варіантах: безконтактна картка або клавіатура та карта. Немає біометричного зчитувача або мобільного телефону. Самі зчитувачі розумні і зберігають більшість даних для системи, що дозволяє їм приймати рішення щодо автентифікації та відкривати двері, навіть якщо мережа не працює. ISONAS дозволяє використовувати сторонні облікові дані зі своєю системою, але він пропонує власні власні облікові дані, включаючи мобільний телефон, картки із значками, теги на шапках, брелоки та тонкі картки.

Однак ISONAS не пропонує певних систем безпеки, які можуть бути важливими складовими комплексної системи контролю доступу. Наприклад, відсутній сигнал пожежі та зупинки. Система дає вам можливість негайно анулювати облікові дані, якщо працівник покидає компанію або виявляє будь-яке зловживання.

Доступ до інтерфейсу звіту системи наявний через веб-браузер на будь-якому пристрої з підключенням до Інтернету, включаючи ноутбуки, планшети та смартфони. Інтерфейс надає докладні звіти про час розблокування, використання облікових даних та підозрілі події. Також можна налаштувати систему проти зворотного зв’язку, щоб вимагати від працівників використання зчитувача виходу, показуючи вам, коли вони входять і виходять.

Березень 2020: ISONAS представив інтерфейс відкритого додатка Pure Access (API), нове програмне забезпечення, яке надає клієнтам справді інтегровану систему безпеки. Відкритий API тепер полегшує постачальникам програмного забезпечення додавати можливості контролю доступу (відеоспостереження, управління обліковими даними, контроль доступу) до своїх існуючих систем безпеки. Pure Access забезпечує повну платформу для встановлення, адміністрування та управління своїм обладнанням для контролю доступу Pure IP.

1.3.3. Johnson Controls

Johnson Controls пропонує послугу керованого доступу, яка виключає повсякденне управління, тому не потрібно чітко керувати системою [7].

Система інтегрується з багатьма іншими аварійними сигналізаціями та системами, такими як спостереження, пожежа та вторгнення.

Пакети Johnson Controls не включають додаткові послуги, такі як облікові дані, вбудовані замки або окремі контрольні точки.

Johnson Controls - це найкращий вибір для підприємств, що мають кілька місцеположень, оскільки його системи легко масштабуються відповідно до будь-якої кількості будівель та дверей. Він також має один з найбільших каталогів продуктів безпеки, тому ви можете створити ідеальну систему для покриття будь-якого місця. Варіанти включають електронні, розміщені, фізичні, керовані та біометричні системи контролю доступу.

Johnson Controls пропонує кілька різних варіантів інтерфейсу для звітності та адміністрування, які охоплюють основи, а потім деякі. Також є можливість керувати системою контролю доступу на смартфоні, що дуже зручно, якщо ви часто перебуваєте далеко від головного офісу [7].

Компанія також пропонує послугу керованого доступу, яка залишає управління вашою безпекою та доступ до Johnson Controls.

Johnson Controls надає високоякісні фізичні дані, а смарт-картки використовують передову технологію шифрування, щоб запобігти клонуванню карт. На додаток до фізичного контролю доступу, Джонсон пропонує розміщений контроль доступу, який зберігає дані в хмарі та легко масштабується та управляється.

Компанія інтегрується з такими системами, як відеоспостереження, пожежна сигналізація, сигналізація про вторгнення, виявлення периметра та відстеження активів. Ці функції можуть бути пов’язані з користувацьким інтерфейсом, дозволяючи налаштувати екстрені процедури, призупинити облікові дані та бути попередженими про підозрілу активність.

Найбільша панель управління може підтримувати до 32 дверей. Якщо потрібно більше дверей, доведеться встановити більше панелей. Однак можна зареєструвати в системі необмежену кількість працівників.

Доступна інтеграція відео означає, що можна витягувати відеокліпи певних подій, таких як підозрілі записи або спроби злому.

Система також дозволяє відстежувати гостей, надаючи відвідувачам тимчасовий доступ та дозволяючи встановлювати рівень їх доступу. Система доступу може бути подвійною в якості відстежувача часу та відвідуваності, повідомляючи вам, коли співробітники приходять та виходять.

Johnson Controls пропонує підтримку та поради на будь-якому етапі процесу, починаючи від проектування та закінчуючи постійним технічним обслуговуванням, а також забезпечує професійну установку електронних, фізичних та біометричних систем.

Листопад 2020: Johnson Controls запустив нову інтелектуальну платформу управління доступом Tyco Illustra Insight. Tyco Illustra розроблений для приміщень з високим трафіком та високою безпекою. Він використовує штучний інтелект та алгоритми навчання, щоб поєднати програмне забезпечення для управління доступом та розпізнавання обличчя для регулювання доступу, забезпечуючи при цьому безпеку [7].

1.3.4. ADT

Пакет ADT включає цілодобовий моніторинг в рамках ADT Security. ADT має мобільний додаток, що дозволяє дистанційно керувати системою контролю доступу [8].

ADT не пропонує біометричних зчитувачів або даних про доступ до мобільних телефонів.

ADT - це вибір в якості найкращої системи відеоспостереження, оскільки пропонуються значні можливості налаштування, що дозволяє розробити систему контролю доступу. Якщо є потреба інтегрувати контроль доступу з іншими функціями безпеки - такими, як моніторинг крадіжок та пожежі, відеоспостереження або дистанційне охоронення та зняття з озброєння - ADT співпрацюватиме із замовником для налаштування рішення безпеки відповідно до ваших потреб.

ADT не пропонує біометричних зчитувачів, а також система не дозволяє доступ до мобільного телефону для працівників, тому ваші співробітники обмежуються використанням карток та PIN-кодів для входу.

ADT також пропонує двосторонній домофон. Існує одне дверне рішення, призначене лише для звуку, яке дозволяє працівникові або відвідувачу поговорити з супроводжуючим. Одна версія не включає механізм звільнення для відвідувачів чи співробітників, але друга версія має цю функцію.

ADT проводить контроль цілодобово. Аварійні служби отримують попередження, коли спрацьовує аварія або пожежна сигналізація, що зручно та економічно ефективно, оскільки вам не потрібно платити додаткові співробітники або наймати зовнішню службу для контролю вашої безпеки [8].

Однією з найпривабливіших функцій системи є її мобільний додаток. За допомогою нього ви можете контролювати майже кожен аспект безпеки свого бізнесу зі свого смартфона. Додаток дозволяє дистанційно блокувати та розблоковувати двері, щоб ви могли впустити працівників, якщо вони забудуть свої повноваження.

1.3.5. Vanderbilt Industries

На додаток до контролю доступу Vanderbilt пропонує відеоспостереження, тому легко інтегрувати дві системи [9]. Система управління дозволяє встановлювати власні сповіщення та віддалено керувати доступом.

Vanderbilt пропонує високоякісне обладнання, яке більш ніж відповідає галузевим стандартам систем контролю доступу, з інтелектуальними зчитувачами дверей та зашифрованими смарт-картами. Vanderbilt – найкращий вибір для підприємств з кількома дверима, оскільки він пропонує системи контролю доступу, які легко масштабувати і не мають обмежень на кількість підтримуваних дверей.

Веб-рішення Vanderbilt для малого та середнього бізнесу, Lite Blue та Bright Blue, дозволяють власникам підприємств негайно заблокувати об'єкт натисканням кнопки [9].

Lite Blue

- Контролює до восьми дверей
- Підтримує до 5000 власників карток
- Легко інтегрується з обладнанням для відеоспостереження та запису

- Яскраво-блакитний

Призначений для середнього бізнесу

- Підтримує до 5000 користувачів карт
- Монітори до 32 дверей
- Інтерфейс, доступний на будь-якому підключеному до Інтернету комп’ютері, із повним журналом історії входів ваших співробітників
- Необмежена пам’ять
- ACT365

Для підприємств, що мають кілька сайтів, таких як роздрібні магазини, тренажерні зали та ресторани

- Забезпечує контроль доступу, а також запис та відтворення відео
- Використовує PIN-коди, ключові картки та брелоки
- Легко інтегрується з управлінням відео
- Підтримує до чотирьох камер на одиницю

За допомогою інтерфейсу звітування та адміністрування ви можете контролювати діяльність своїх співробітників і налаштовувати сповіщення про будь-яку діяльність, яка вважається підозрілою. Всі системи Vanderbilt дають повний контроль над безпекою вашої будівлі. Можна легко активувати та деактивувати доступ для співробітників та інших. Сигналізація пожежі та вторгнення Вандербільта може бути підключена до системи для більш повного охоплення.

Vanderbilt також пропонує систему управління безпекою, яка інтегрує технології контролю доступу вашого об'єкта з цифровими системами відеоспостереження та сигналізації, що дозволяє управляти всією безпекою на одній платформі.

Жовтень 2020: Vanderbilt Industries представила Mobile Act ID, хмарну опцію облікових даних із нульовим дотиком, яка дозволяє адміністраторам легко контролювати доступ та автентифікувати користувачів за допомогою хмари. Облікові дані легко інтегруються з усіма платформами контролю доступу Vanderbilt і не вимагають додаткових підписок або зборів. Ця функція дозволяє користувачам швидко видавати нові облікові дані та надавати та обмежувати доступ до об'єктів [9].

1.4. Висновки до розділу 1

Проведено аналіз існуючих методів контролю доступу для приміщень, їх переваги та недоліки. Проведено огляд систем контролю доступу та наявний стан ринку.

На основі проведеного аналізу можна зробити висновок, що системи контролю доступу це складні та багатокомпонентні системи. Також неможливо створити універсальну систему, що буде задовольняти потреби малого, середнього та великого бізнесу, а також потреби фізичних осіб. Тому перспективним вбачається метод, що грунтується на аналізі даних з наявних систем контролю доступу із застосуванням методів штучного інтелекту для реалізації механізму виявлення загроз та небезпечних ситуацій.

РОЗДІЛ 2 Розробка архітектури виявлення загроз в системі контролю доступу

В даному розділі будуть розглянуті методи для аналізу даних з наявних систем контролю доступу із застосуванням методів штучного інтелекту для реалізації механізму виявлення загроз та небезпечних ситуацій.

2.1. Методи інтелектуального аналізу даних

Інтелектуальний аналіз даних (ІАД) є галуззю досліджень, що дає змогу виділити деяку нову значущу інформацію у великому обсязі даних [10]. Головним завданням цієї галузі є отримання явно не видимих зв'язків і непередбачених тенденцій з допомогою різних методів обробки даних. Залежно від використаних принципів роботи з вихідними навчальними даними все методи ІАД поділяються на дві великі групи. Дві ці групи й параметри методів, що входять до їх складу, представлені на рис 2.1.

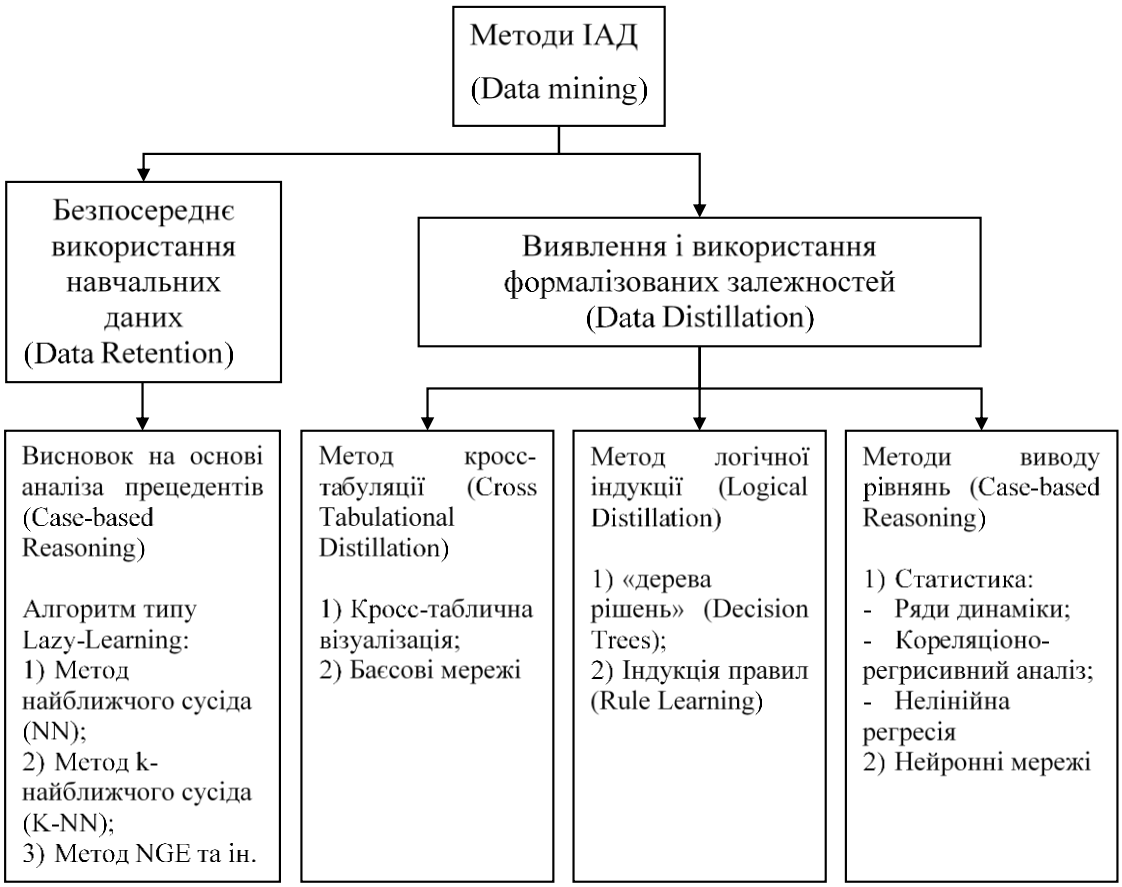

Рис.2.1. Класифікація технологічних методів ІАД [10]

Як видно з рис.2.1 до базових методів ІАД відносять насамперед алгоритми, засновані на перебиранні. Оптимізація подібних алгоритмів зводиться до приведення залежності кількості операцій від кількості досліджуваних даних у функції лінійного виду. Водночас залежність від кількості атрибутів, як правило, залишається експоненційною. За умови, що їх небагато (в переважній більшості випадків їх значно менше, ніж даних), така залежність є прийнятною.

Також можна розділити методи ІАД на описові й ті, що прогнозують [11]. Описові методи мусять призводити до пояснення або поліпшення розуміння даних. Ключовий момент у таких моделях – легкість і прозорість сприйняття дослідником одержуваних результатів. До таких завдань належать класичні методи перевірки статистичних гіпотез, кластеризація й пошук асоціативних правил.

Завдання аналізу даних можна звести до задачі вибору функції $y(x_i)$ з мінімальним ступенем помилки:

$$\min_{\psi \in \Psi} R(\psi) = \frac{1}{m} \sum_{i=1}^{m} C[y_i, \psi(x_i)],$$

де Ψ – безліч усіх можливих функцій; $C[y_i, \psi(x_i)]$ – функція втрат, в якій $\psi(x_i)$ – значення залежної змінної, знайдене за допомогою функції ψ для вектора x_i, а y – її точне (відоме) значення.

Для бінарної класифікації (належність об’єкта до одного з двох класів) найпростіша функція втрат у разі неправильного передбачення приймає значення 1 і 0 – в іншому випадку. Ситуація ускладнюється при числі класів понад два. Кожен тип помилки класифікації вносить свій тип втрат і в загальному випадку виходить матриця вартостей помилок k×k (де k – число класів). У завданнях регресії найчастіше застосовується мінімізація квадратів різниць $\psi(x_i) - y_i$, що відповідає наявності адитивного нормально розподіленого шуму, що впливає на результати спостережень y_i. Проте більш стійкі оцінки отримують не мінімізацією квадратів різниць, а мінімізацією степені 1.6 різниць, тобто min $[(y(x]_i) - y_i)^{1.6}$.

Основною перевагою алгоритмів перебирання є їх простота, як із погляду розуміння, так і реалізації. До недоліків можна віднести брак формальної теорії, на базі якої будуються такі алгоритми, і, також складнощі, пов'язані з їх дослідженням і розвитком.

Виділяють такі етапи, які супроводжують рішення завдань ІАД:

1. Аналіз предметної сфери, формулювання цілей і завдань дослідження;
2. Витяг і збереження даних;
3. Попередня обробка даних: очищення, інтеграція, перетворення;
4. Аналіз даних методами Data Mining;
5. Інтерпретація отриманих результатів;
6. Використання нових знань для прийняття рішень.

2.2. Машинне навчання

Машинне навчання являє собою клас методів штучного інтелекту, для якого характерно непряме рішення завдання, а навчання в процесі застосування рішень безлічі подібних завдань [12, 13]. У процесі побудови таких методів можуть бути використані засоби математичної статистики, чисельних методів, методів оптимізації, інтелектуального аналізу даних, теорії ймовірностей, теорії графів.

За допомогою машинного навчання можливе вивчення закономірностей у даних, які згодом використовуються для виявлення аномальної поведінки. Завдання машинного навчання зазвичай поділяються на такі категорії залежно від наявності навчального «сигналу» або «зворотного зв'язку», доступного для системи навчання:

- Навчання з вчителем за допомогою прикладів «реакція-стимул»;
    - Часткове навчання з вчителем;
    - Активне навчання;
    - Навчання з підкріпленням;
- Навчання без вчителя, підходить для задач у якій об'єкти детально описані та треба встановити внутрішні взаємозв'язки між об'єктами.

Процес машинного навчання вимагає достатньої кількості даних, відповідних як нормального режиму роботи системи, так і аномальним ситуацій. Тому, як варі-

ант, машинне навчання може здійснюватися на змодельованих наборах даних за участю експерта.

Існує кілька основних алгоритмів для побудови і навчання моделей класифікаторів, які можна застосувати для вирішення завдання виявлення загроз [13]. Розглянемо деякі з них детальніше.

2.2.1. Метод k найближчих сусідів

Робота даного методу грунтується на зберіганні даних в пам'яті для порівняння з новими елементами. При появі нової події в системі для прогнозування знаходяться відхилення між цією подією і подібним набором даних, і найбільш подібна подія (або найближчий сусід) ідентифікується. При такому підході використовується термін k-найближчих сусідів. Термін означає, що вибирається k верхніх (найближчих) сусідів для їх розгляду в якості безлічі найближчих сусідів. Оскільки не завжди зручно зберігати всі дані, іноді зберігається тільки безліч типових випадків. В такому випадку використовується метод називають міркуванням за аналогією (Case Based Reasoning, CBR), міркуванням на основі аналогічних випадків, міркуванням по прецедентах [20].

Переваги методу:

- простота використання отриманих результатів;
- рішення не унікальні для конкретної ситуації, їх використання можливе для інших випадків;
- метою пошуку є не гарантовано вірне рішення, а найкраще з можливих.

Недоліки методу:

- не створює моделі і правила;
- неможливість точного визначення підстави на якому було прийнято рішення;
- висока залежність результатів класифікації від обраної метрики;
- обчислювальна трудомісткість;
- добре застосовні лише для задач з невеликою розмірністю.

2.2.2. Динамічні байєсовські мережі

Байєсова мережу (БМ) - це графічна модель, що представляє собою безліч змінних і їх імовірнісних залежностей. БМ є чудовим інструментом для опису досить складних процесів і подій з невизначеностями. БМ виявилася особливо корисною при розробці та аналізі машинних алгоритмів навчання. Основною ідеєю побудови графічної моделі є поняття модульності, тобто розкладання складної системи на прості елементи. Для об'єднання окремих елементів в систему використовуються результати теорії ймовірностей. Динамічні байєсовські мережі є узагальненою моделлю в просторі станів. Назва динамічні вказує не на залежність структури від часу, а тільки на залежність від моделювання процесу [20].

Переваги байесовских мереж:

- в моделі визначаються залежно між усіма змінними, це дозволяє легко обробляти ситуації, в яких значення деяких змінних невідомі;
- дозволяють на етапі прогностичного моделювання легко проводити аналіз за сценарієм що, якщо;
- байесовский метод дозволяє природним чином поєднувати закономірності, виведені з даних;
- які не піддаються проблеми переучування.

Байєсівський підхід має наступні недоліки:

- перемножать умовні ймовірності коректно тільки тоді, коли всі вхідні змінні дійсно статистично незалежні, хоча часто цей метод показує досить хороші результати при недотриманні умови статистичної незалежності, але теоретично така ситуація повинна оброблятися більш складними методами, заснованими на навчанні байесовских мереж;
- неможлива безпосередня обробка безперервних змінних;
- на результат впливають тільки індивідуальні значення вхідних змінних, комбінований вплив пар або трійок значень різних атрибутів тут не враховується.

2.2.3. Нейронні мережі

Нейронні мережі - це моделі біологічних нейронних мереж мозку, в яких нейрони імітуються відносно простими, часто однотипними, елементами (штучними нейронами). Нейронна мережа може бути представлена спрямованим графом з зваженими зв'язками, в якому штучні нейрони є вершинами, а синаптичні зв'язки – дугами [20].

Серед областей застосування нейронних мереж - автоматизація процесів розпізнавання образів, прогнозування, адаптивне управління, створення експертних систем, організація асоціативної пам'яті, обробка аналогових і цифрових сигналів, синтез і ідентифікація електронних ланцюгів і систем.

За допомогою нейронних мереж вирішуються наступні завдання машинного навчання:

- класифікація (навчання з учителем). Приклади завдань класифікації: розпізнавання тексту, розпізнавання мови, ідентифікація особистості;
- прогнозування. Для нейронної мережі задача прогнозування може бути поставлена таким чином: знайти найкраще наближення функції, заданої кінцевим набором вхідних значень (навчальних прикладів). Наприклад, нейронні мережі дозволяють вирішувати завдання відновлення пропущених значень;
- кластеризація (навчання без вчителя). Прикладом завдання кластеризації може бути задача стиснення інформації шляхом зменшення розмірності даних. Завдання кластеризації вирішуються, наприклад, до самоорганізації картами Кохонена.

Недоліки нейронних мереж:

- складність може викликати питання про кількість спостережень в наборі даних. І хоча існують якісь правила, що описують зв'язок між необхідною кількістю спостережень і розміром мережі, їх вірність не доведена;

- кількість необхідних спостережень залежить від складності розв'язуваної задачі. При збільшенні кількості ознак кількість спостережень зростає нелінійно;
- аналітик повинен визначити кількість шарів у мережі і кількість нейронів в кожному шарі. Алгоритму вибору оптимальної структури до цих пір не існує;
- часто виникає проблема перенавчання.

Перенавчання, або надмірно близька підгонка - зайве точну відповідність нейронної мережі конкретному набору навчальних прикладів, при якому мережу втрачає здатність до узагальнення. Перенавчання пов'язано з тим, що вибір навчального (тренувального) безлічі є випадковим. З перших кроків навчання відбувається зменшення помилки. На наступних кроках з метою зменшення помилки (цільової функції) параметри підлаштовуються під особливості навчальної множини. Однак при цьому відбувається підстроювання не під загальні закономірності ряду, а під особливості його частини - навчає підмножини. При цьому точність прогнозу зменшується.

2.2.4. Метод опорних векторів

Це математичний метод отримання функції, вирішує завдання класифікації. Ідея методу виникла з геометричною інтерпретації завдання класифікації [20]. У 90-х рр. минулого століття метод МОВ був удосконалений: розроблені ефективні алгоритми пошуку оптимальної площини, знайдені способи узагальнення на нелінійні випадки і ситуації з числом класів, великим двох.

Переваги методу МОВ:

- метод опорних векторів, на відміну від нейронних мереж, стійкий до перенавчання. Даний алгоритм може навчатися на вибірці розміром в гігабайти вихідних даних, сильно корелюють між собою;
- робота з високою розмірністю вхідних векторів;

- конкурентоспроможність в порівнянні з методами, заснованими на інших алгоритмах.

Недоліки методу SVM:

- нестійкий по відношенню до шуму у вихідних даних;
- до сих пір не розроблені загальні методи побудови спрямляющий просторів або ядер, найбільш придатних для конкретного завдання.

2.2. База даних Time & Space

База даних Time & Space є комерційним продуктом компанії Špica International для контролю доступу та контролю часу [21]. Для цілей нашого дослідження, база даних Time & Space потребувала незначних модифікацій. Зокрема, був реалізований більш детальний запис часу від вхідних датчиків. По суті, всі інші функції, такі як масштабованість, модульність та безпека, залишились тими самими, що дозволило створити надійну та гнучку базу даних.

Атрибут	Опис
X1={0|1|X}	Ознака робочого часу
X2={0|1|X}	Перше відвідування об'єкта
X3={0:n|X}	Рівень доступу карти
X4={0:n|X}	Рівень доступу об'єкта
X5={0|1|X}	Спроба завантажити забороненого об'єкта
X6={0:n|X;Obj;L}	Кількість спроб доступу; об'єкт; рівень доступу об'єкта
X7={0|1|X;Obj;L}	Ознака відмови обладнання; об'єкт; рівень доступу об'єкта
X8={0:n|X}	Множинний вхід в різні об'єкти без виходу
X9={0|1|X;Obj;L}	Відключення електроживлення; об'єкт; рівень доступу об'єкта
X10={0|1|X;Obj;L}	Відкриття дверей, без події проходу; об'єкт; рівень доступу об'єкта
X11={0|1|X;Obj;L}	Чи не замкнені двері; об'єкт; рівень доступу об'єкта

X12={0|1|X}	Доступ всередині об'єкту, що охороняється, без проходу на територію підприємства

2.3. Експертно визначені правила

Навіть існуючі системи комерційного доступу використовують кілька правил для контролю базової поведінки на макрорівні. Такі правила описують, наприклад, максимальний час, коли двері можуть бути відчинені, або якщо людина може зайти в будівлю в суботу. На додаток до врахування цих "загальних" правил, зібрано нові правила, проконсультувавшись із експертом з питань безпеки. Завдяки набуттю знань ми отримали достатньо інформації, щоб розробити загалом дев'ять шаблонів правил. Кожен шаблон правила повинен бути заповнений точними даними за допомогою редактора правил. В результаті можна створити кілька або кілька десятків конкретних правил. Деякі правила досить прості, тоді як інші вимагають належного виконання спеціалізованих змінних та процедур. Прикладом шаблону правила є: Модуль запускає ПОВІДОМЛЕННЯ, якщо користувачі SET_USERS не виходять із будівлі в часі TIME_LIMIT. MESSAGE може бути як попередженням, так і сигналом тривоги, тоді як TIME_LIMIT - це ціле значення, що вимірюється в секундах. SET_USERS - це приклад спеціальної процедури, яка дозволяє вибрати конкретного користувача, певну групу користувачів або всіх користувачів системи. Це правило, очевидно, вимагає спеціального ручного кодування, яке перевіряє всіх людей, які увійшли до будівель і не вийшли, і порівнює час, проведений у будівлі, з TIME_LIMIT. Правила в поточному впровадженні не пов'язані, як у типовому експерті чи системі, що базується на правилах. Швидше за все, механізм виведення перевіряє всі правила у списку одне за одним і запускає повідомлення в тих правилах, які відповідають передумовам. Правила перетворюються на запити SQL і виконуються в базі даних Time & Space. Якщо якесь правило викликає попередження (або сигнал тривоги), класифікація всього модуля є попередженням (або сигналом тривоги) [22].

2.4. Програмні системи для навчання нейронних мереж

Нині створена велика кількість програмних систем для навчання глибоких нейронних мереж. Серед найбільш популярних із них можна зазначити Caffe, Theano, TensorFlow, Torch. Їх основні характеристики приведені в таблиці 2.1.

Таблиця 2.1. Програмне забезпечення для навчання глибоких нейронних мереж

Назва	Платформа	Мова	Інтерфейс	Підтримка OpenMP	Підтримка OpenCL	Підтримка CUDA	Авто диферн-ціювання	Містить треновані моделі	Рекурентні мережі	Згорткові мережі	Паралельне виконання (багато-вузлове)
Apache Singa	Linux, Mac OS X, Windows	C++	Python, C++, Java	Ні	Так	Так	Ні	Так	Так	Так	Так
Caffe	Linux, Mac OS X, Windows	C++	Python, MATLAB	Так	Ні	Так	Так	Так	Так	Так	Ні
Deeplearning4j	Linux, Mac OS X, Windows, Android (багатоплатформне)	Java	Java, Scala, Clojure, P ython (Keras)	Так	Ні	Так	Так	Так	Так	Так	Так
Dlib	багатоплатформне	C++	C++	Так	Ні	Так	Так	Так	Ні	Так	Так
Keras	Linux, Mac OS X, Windows	Python	Python	Так	Ні	Так	Так	Так	Так	Так	Так
Microsoft Cognitive Toolkit	Windows, Linux	C++	Python, C++	Так	Ні	Так	Так	Так	Так	Так	Так
MXNet	Linux, Mac OS X, Windows, Android, iOS	C++	C++, Python, Julia, Ma tlab, JavaScript, Go, R, Scala, Perl	Так	Ні	Так	Так	Так	Так	Так	Так
Neural Designer	Linux, Mac OS X, Windows	C++	Графічний інтерфейс к	Так	Ні	Ні	Ні	Ні	Ні	Ні	Ні
OpenNN	багатоплатформне	C++	C++	Так	Ні	Ні	Ні	Ні	Ні	Ні	Ні
TensorFlow	Linux, Mac OS X, Windows	C++, Python	Python, C/C++, Java, Go	Ні	Ні	Так	Так	Так	Так	Так	Так
Theano	багатоплатформне	Python	Python	Так	Ні	Так	Так	Ні	Так	Так	Так
Torch	Linux, Mac OS X, Windows, Android, iOS	C, Lua	Lua, LuaJIT, C, C++/OpenCL	Так	Ні	Так	Так	Так	Так	Так	Так
Mathematica	Windows, Mac OS X, Linux	C++	Java, C++	Ні	Так	Так	Так	Так	Так	Так	Так

Експериментальні дослідження проводились із використанням мови програмування Python та з використання бібліотек чисельного обчислення Theano та глибинного навчання Keras і Tensorflow.

Theano забезпечує високу продуктивність внаслідок того, що програма на Python автоматично перетворюється в програму на C++, що компілюється й потім виконується. TensorFlow включає системи ефективної роботи з тензорами й потокової обробки даних на графі. Keras надає зручний і простий у використанні програм-

ний інтерфейс для навчання глибоких нейронних мереж. Keras не є самостійною системою, а працює поверх Theano, TensorFlow або CNTK [22-25].

2.5. Висновки до розділу 2

Розглянуто методи інтелектуального аналізу даних. Наведено переваги та недоліки методів машинного навчання. Обгрунтовано використання нейронних мереж для поставленної задачі, яка полягає в виявленні загроз та небезпечних ситуацій.

Для розробки апаратно-програмного макету було використоване сучасне програмне забезпечення, а саме PyCharm для програмування на python та бібліотеками чисельного обчислення Theano та глибинного навчання Keras і Tensorflow.

РОЗДІЛ 3 Алгоритмичне забезпечення

3.1. Алгоритм запропонованого методу СКД

Розглянувши основні методи вирішення поставленого завдання, прийнято рішення реалізувати механізм виявлення загрози застосовуючи метод Random Forest (випадкових лісів) [26]. Математична модель являє собою ансамбль бінарних дерев рішень, побудованих на навчальної бутстреп вибірці по усеченному набору параметрів.

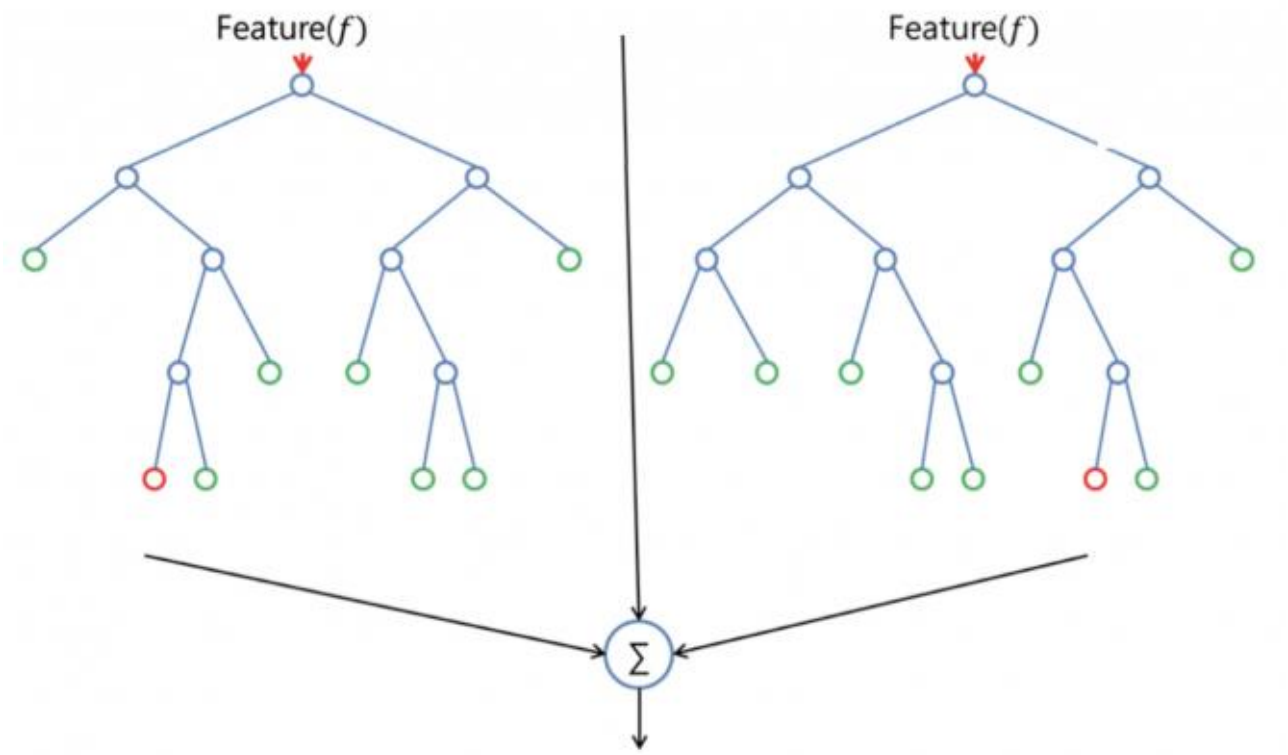

Рис.3.1. Узагальнений приклад алгоритму Random Forest із двома деревами.

Алгоритм навчання для випадкових лісів застосовує загальну техніку агрегування завантажувального бутстрапа, який навчається на деревах. Враховуючи навчальний набір $X = x_1, ..., x_n$ із відповідями $Y = y_1, ..., y_n$, багаторазове завантаження (B разів) відбирає випадкову вибірку із заміною навчального набору та підбирає дерева до цих зразки:

Для $b = 1, ..., B$:

1. Зразок із заміною, n навчальних прикладів з X , Y ; назвемо їх X_b , Y_b .
2. Навчіть дерево класифікації або регресії f_b на X_b , Y_b .

Після тренування прогнози для невидимих зразків x' можуть бути зроблені шляхом усереднення прогнозів з усіх окремих дерев регресії на x':

$$\hat{f} = \frac{1}{B}\sum_{b=1}^{B} f_b(x')$$

або шляхом прийняття більшості голосів у випадку дерев класифікації.

Ця процедура завантаження призводить до кращої продуктивності моделі, оскільки вона зменшує дисперсію моделі, не збільшуючи зміщення. Це означає, що, хоча передбачення окремого дерева дуже чутливі до шуму в його навчальному наборі, середнє значення для багатьох дерев не є, доки дерева не співвідносяться. Просто тренування багатьох дерев на одному навчальному наборі дасть сильно корельовані дерева (або навіть одне і те ж дерево багато разів, якщо алгоритм навчання детермінований); вибірка початкового завантаження - це спосіб зняти кореляцію між деревами, показуючи їм різні навчальні набори [20].

Крім того, оцінка невизначеності прогнозу може бути зроблена як стандартне відхилення передбачень від усіх окремих дерев регресії на x':

$$\sigma = \sqrt{\frac{\sum_{b-1}^{B}(f_b(x') - \hat{f})^2}{B-1}}.$$

Кількість зразків або дерев, B, є вільним параметром. Зазвичай використовується від декількох сотень до кількох тисяч дерев, залежно від розміру та характеру навчального набору. Оптимальну кількість дерев B можна знайти за допомогою перехресної перевірки або шляхом спостереження помилки, що вийшла з мішка: середньої помилки прогнозування для кожної навчальної вибірки x_i, використовуючи лише дерева, які не мали x_i у своїй вибірці завантажувального ремесла. Помилки в навчанні та тестуванні, як правило, вирівнюються після того, як певна кількість дерев підходить.

Хоча random forest – це сукупність дерев рішень, є деякі відмінності.

Якщо вводиться навчальний набір даних із функціями та мітками у дерево рішень, він сформулює певний набір правил, які будуть використані для прогнозуван-

ня. Інша відмінність полягає в тому, що дерева "глибоких" рішень можуть постраждати від перенавчання. Найчастіше random forest запобігає цьому, створюючи випадкові підмножини об’єктів та будуючи менші дерева за допомогою цих підмножин. Потім він поєднує піддерева.

Однією з найбільших переваг random forest є його універсальність. Він може бути використаний як для регресії, так і для завдань класифікації, а також легко переглянути відносну важливість, яку він надає вхідним ознакам.

Random forest також є дуже зручним алгоритмом, оскільки гіперпараметри за замовчуванням, які він використовує, часто дають хороший результат прогнозування.

Однією з найбільших проблем машинного навчання є перенавчання, але здебільшого це не відбувається завдяки випадковому класифікатору лісів. Якщо в лісі достатньо дерев, класифікатор не перенавчить модель.

Основне обмеження random forest полягає в тому, що велика кількість дерев може зробити алгоритм занадто повільним та неефективним для прогнозів у реальному часі. Взагалі, ці алгоритми швидко тренуються, але досить повільно створюють прогнози після того, як їх навчать. Для більш точного прогнозування потрібно більше дерев, що призводить до уповільнення моделі. У більшості реальних додатків алгоритм випадкового лісу досить швидкий, але, безумовно, можуть бути ситуації, коли продуктивність виконання є важливою, і інші підходи будуть кращими.

І, звичайно, random forest є інструментом прогнозуючого моделювання, а не інструментом опису, тобто якщо ви шукаєте опис взаємозв’язків у ваших даних, інші підходи були б кращими.

Алгоритм роботи математичної моделі представлений на рис.3.2.

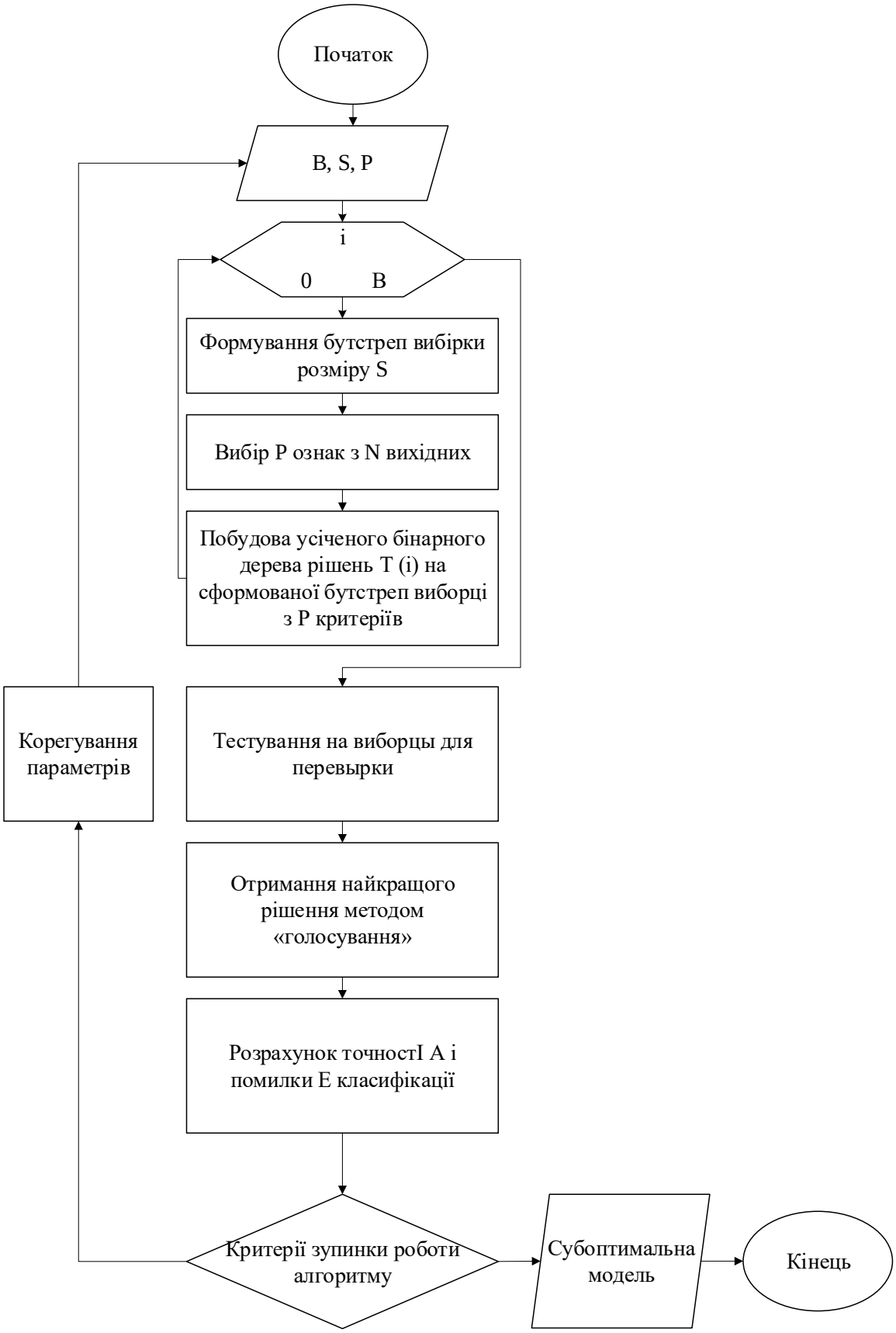

Рис.3.2. Алгоритм запропонованого методу

3.2. Розробка програмного забезпечення для навчання нейронної мережі

Ініціалізація датасету зображена на рис.3.2.

```python
# import packages
import math

import tensorflow as tf
from tensorflow import keras
from tensorflow.keras import layers
from tensorflow.keras.utils import Sequence
from datetime import timedelta
from sklearn.preprocessing import MinMaxScaler
from sklearn.metrics import mean_squared_error

import numpy as np
import pandas as pd
import time

import os

# read the dataset into python
df = pd.read_csv('power_temp_dataset.txt',
delimiter=';')
df.head()
```

Рис.3.2. Завантаження датасету

Крок 1. Передобробка датасету для аналізу часових рядів (рис.3.3)

Датасет df оброблюється наступним чином:

- Створюється функція date_time у форматі DateTime (поєднання дати та часу);
- Перетворення Active_temp в числове значення та видалення пропущених значень;
- Упорядкування об’єктів за часом у новому наборі даних.

```
%%time

# This code is copied from https://towardsdatascience.com/time-series-analysis-visualization-forecasting-with-lstm-77a905180eba
# with a few minor changes.
#
df['date_time'] = pd.to_datetime(df['Date'] + ' ' + df['Time'])
df['Active_temp '] = pd.to_numeric(df['Active_temp '], errors='coerce')
df = df.dropna(subset=['Active_temp '])

df['date_time'] = pd.to_datetime(df['date_time'])

df = df.loc[:, ['date_time', 'Active_temp ']]
df.sort_values('date_time', inplace=True, ascending=True)
df = df.reset_index(drop=True)

print('Number of rows and columns after removing missing values:', df.shape)
print('The time series starts from: ', df['date_time'].min())
print('The time series ends on: ', df['date_time'].max())
```

Рис.3.3. Передобробка датасету для аналізу часових рядів

Далі датасет розбивається на набори даних для навчання, перевірки та тестування (рис.3.4).

– df_test зберігає дані за останні 2 місяці у вихідному наборі даних;
– df_val має дані за 3 місяців до тестового набору даних;
– df_train містить інші дані.

```
# Split into training, validation and test datasets.
# Since it's timeseries we should do it by date.
test_cutoff_date = df['date_time'].max() -
timedelta(month=13)
val_cutoff_date = test_cutoff_date -
timedelta(month=10)

df_test = df[df['date_time'] > test_cutoff_date]
df_val = df[(df['date_time'] > val_cutoff_date) &
(df['date_time'] ⩽ test_cutoff_date)]
df_train = df[df['date_time'] ⩽ val_cutoff_date]

#check out the datasets
print('Test dates: {} to
{}'.format(df_test['date_time'].min(),
df_test['date_time'].max()))
print('Validation dates: {} to
{}'.format(df_val['date_time'].min(),
df_val['date_time'].max()))
print('Train dates: {} to
{}'.format(df_train['date_time'].min(),
df_train['date_time'].max()))
```

Рис.3.4. Розбиття датасету на набори даних

Крок 2. Перетворення набору даних для TensorFlow Keras.

Треба визначити клас об’єкту часового ряду, створюється клас TimeSeriesLoader для перетворення та передачі фреймів даних у модель (рис.3.5.). У цьому класі ми визначаємо:

- __init__: початкові налаштування об’єкта, включаючи:
  - ts_folder, який буде ts_data, який ми тільки що створили.
  - filename_format, який являє собою строковий формат імен файлів в ts_folder.
- num_chunks: загальна кількість файлів (блоків).
- get_chunk: цей метод бере фрейм даних з одного з файлів, обробляє його для підготовки до навчання.
- shuffle_chunks: цей метод перемішує порядок блоків, які повернуться в get_chunk.

```
#

class TimeSeriesLoader:
    def __init__(self, ts_folder, filename_format):
        self.ts_folder = ts_folder

        # find the number of files.
        i = 0
        file_found = True
        while file_found:
            filename = self.ts_folder + '/' +
filename_format.format(i)
            file_found = os.path.exists(filename)
            if file_found:
                i += 1

        self.num_files = i
        self.files_indices = np.arange(self.num_files)
        self.shuffle_chunks()

    def num_chunks(self):
        return self.num_files

    def get_chunk(self, idx):
        assert (idx >= 0) and (idx < self.num_files)

        ind = self.files_indices[idx]
        filename = self.ts_folder + '/' +
filename_format.format(ind)
        df_ts = pd.read_pickle(filename)
        num_records = len(df_ts.index)

        features = df_ts.drop('y', axis=1).values
        target = df_ts['y'].values

        # reshape for input into LSTM. Batch major
format.
        features_batchmajor =
np.array(features).reshape(num_records, -1, 1)
        return features_batchmajor, target

    # this shuffles the order the chunks will be
outputted from get_chunk.
    def shuffle_chunks(self):
        np.random.shuffle(self.files_indices)
```

Рис.3.5. Перетворення набору даних для TensorFlow Keras

Далі TimeSeriesLoader застосовується до ts_data (рис.3.6)

```
ts_folder = 'ts_data'
filename_format = 'ts_file {}. pkl'
tss = TimeSeriesLoader ( ts_folder , filename_format
)
```

Рис.3.6. Застосування TimeSeriesLoader для перетворення та передачі фреймів даних у модель

Крок 3. Створення моделі RandomForest

Модель RandomForest будується на основі бібліотеки TensorFlow Keras (рис.3.7).

Далі виконуються такі процедури:

- визначення форми вхідного набору даних:
  - num_timesteps, кількість затримок у фреймах даних.
  - кількість часових рядів дорівнює 1, оскільки використовується тільки одна функція Active_temp.
- визначення кількості юнітів, 4*юніт*(юніт + 2) – це кількість параметрів RandomForest. Чим більше юніт, тим більше параметрів у моделі.
- визначення частоти відсіву, яка використовується для запобігання перенавчання.
- визначення вихідного шару для лінійної функції активації.
- визначення моделі.

```
ts_inputs = tf.keras.Input(shape=(num_timesteps, 1))
x = layers.LSTM(units=10)(ts_inputs)
x = layers.Dropout(0.2)(x)
outputs = layers.Dense(1, activation='linear')(x)
model = tf.keras.Model(inputs=ts_inputs,
outputs=outputs)
```

Рис.3.7. Створення моделі RandomForest на основі бібліотеки TensorFlow Keras

Далі визначаються функції оптимізації та втрат (рис.3.8)

```
model.compile(optimizer=tf.keras.optimizers.SGD(learning_rate=0.01),
              loss=tf.keras.losses.MeanSquaredError(),
              metrics=['mse'])
```

Рис.3.8. Визначення функції оптимізації та витрат

Кожен фрагмент набору даних навчається групами і виконується тільки одна епоха (рис.3.9).

```
%%time

BATCH_SIZE = 128
NUM_EPOCHS = 1
NUM_CHUNKS = tss.num_chunks()

for epoch in range(NUM_EPOCHS):
    print('epoch #{}'.format(epoch))
    for i in range(NUM_CHUNKS):
        X, y = tss.get_chunk(i)
        model.fit(x=X, y=y, batch_size=BATCH_SIZE)

    tss.shuffle_chunks()
```

Рис.3.9. Групування наборів даних

Після підбору моделі оцінюється її продуктивність, використовуючи набір даних для перевірки (рис.3.10).

```
Active_temp_val = df_val['Active_temp'].values
Active_temp_val_scaled =
scaler.transform(Active_temp_val.reshape(-1,
1)).reshape(-1, )

history_length = 7*24*60*60
step_size = 10
target_step = 10
num_timesteps =
create_ts_files(Active_temp_val_scaled,
                  start_index=0,
                  end_index=None,
                  history_length=history_length,
                  step_size=step_size,
                  target_step=target_step,
                  num_rows_per_file=128*100,
                  data_folder='ts_val_data')
```

Рис.3.10. Оцінка продуктивності моделі

Окрім тестування моделі з використанням набору даних для перевірки, модель тестується на основі базової моделі, використовуючи тільки останню точку часового ряду (рис.3.11).

```
df_val_ts = pd.read_pickle('ts_val_data/ts_file0.pkl')

features = df_val_ts.drop('y', axis=1).values
features_arr = np.array(features)


num_records = len(df_val_ts.index)
features_batchmajor =
features_arr.reshape(num_records, -1, 1)

y_pred =
model.predict(features_batchmajor).reshape(-1, )
y_pred = scaler.inverse_transform(y_pred.reshape(-1,
1)).reshape(-1 ,)

y_act = df_val_ts['y'].values
y_act = scaler.inverse_transform(y_act.reshape(-1,
1)).reshape(-1 ,)

print('validation mean squared error:
{}'.format(mean_squared_error(y_act, y_pred)))

#baseline
y_pred_baseline = df_val_ts['x_lag11'].values
y_pred_baseline =
scaler.inverse_transform(y_pred_baseline.reshape(-1,
1)).reshape(-1 ,)
print('validation baseline mean squared error:
{}'.format(mean_squared_error(y_act,
y_pred_baseline)))
```

Рис.3.11. Тестування на основі базової моделі

```
dt = DecisionTreeClassifier(min_samples_split=15, min_samples_leaf=20,
random_state=42)
dt.fit(X_train, Y_train)
dt_prediction = dt.predict(X_test)

score = metrics.accuracy_score(Y_test, dt_prediction)
display_confusion_matrix(Y_test, dt_prediction, score=score)
print(score)
scores.append(score)
print(scores)
```

Рис.3.12. Верифікація моделі

Простим показником ефективності моделі являється точність, доля правильних прогнозів во всьому наборі даних тестування, що визначається як:

$$ACC_C = \frac{TP_C + TN_C}{n}$$

Також для оцінювання алгоритму моделі використовуються такі метрики, як прецизійність і повнота. Точність у межах класу – це доля об'єктів, що дійсно належать даному класу відносно всіх об'єктів, які система віднесла до даного класу, вона визначається як:

$$Precision_C = \frac{TP_C}{TP_C + FP_C} = \frac{TP_C}{P_C}$$

Повнота системи – це доля знайдених класифікатором об'єктів, що належать до класу відносно всіх об'єктів даного класу в тестовій вибірці, вона визначається як:

$$Recall_C = \frac{TP_C}{TP_C + FN_C} = \frac{TP_C}{S_C}$$

Результуюча точність класифікатора розраховується як середнє арифметичне його точності по всіх класах. Те ж саме з повнотою. Технічно цей підхід називається macro-averaging.

Середнє гармонічне значення прецизійності та повноти визначає показник F-міра:

$$F_c = 2 \cdot \frac{Precision_C \cdot Recall_C}{Precision_C + Recall_C}$$

Дана формула надає однакову вагу точності й повноти, тому F-міра буде падати однаково при зменшенні й точності й повноти.

	0	1	Точність	Макспо середнє	Взважене середнє
Прецизійність	0.98	0.82	0.96	0.90	0.96
Повнота	0.98	0.84	0.96	0.91	0.96
Ф-міра	0.98	0.83	0.96	0.91	0.96
Кількість об’єктів, що належать класу	1604.00	196.00	0.96	1800.00	1800.00

Рис.3.13. Представлення результатів верифікації моделі у вигляді факторної таблиці

3.3. Висновки до розділу 3

Описано робота методу Random Forest, його переваги та недоліки. Розроблено алгоритмічне забезпечення та наведено покрокове пояснення навчання нейронної мережі. Проведена верифікація нейроної мережі, результати представлені у вигляді факторної таблиці.

РОЗДІЛ 4 Охорона навколишнього середовища

4.1. Аналіз впливу інформаційних технологій на навколишнє середовище

Ключовими чинниками, що впливають на навколишне середовище з класу інформаційних технологій є:

- Обладнання кінцевого користувача (комп'ютери, планшети, ноутбуки, маршрутизатори);
- Центри обробки даних (які зберігають та розміщують веб-сторінки);
- Мережі доступу (електропроводка та антени, що передають дані).

Різні джерела наводять різні висновки щодо впливу інтернету на навколишнє середовище. Так 2010 р. The Guardian навів цифру в 300 млн.т. CO2 на рік – «стільки, скільки всього вугілля, нафти та газу спалювалося в Туреччині чи Польщі за один рік». В статті «Сила, забруднення та Інтернет» в The New York Times показано цифру в 30 мільярдів ват електроенергії в 2011 році, "приблизно еквівалентну потужності 30 атомних електростанцій". Консультанти Gartner повідомляли, що Інтернет відповідав за 2% глобальних викидів у 2007 році, випередивши вуглецевий слід авіаційної галузі. Дослідження, проведене в 2013 році дослідницьким центром CEET з Мельбурна, підрахувало, що телекомунікаційна галузь в цілому викидає 830 мільйонів тонн вуглекислого газу на рік, і що енергетичні потреби Інтернету можуть подвоїтися до 2020 року [27].

За розрахунками Джона Кумі використання електроенергії всіма елементами, що складають Інтернет, становить, близько 10% від загального споживання електроенергії. Хоча розрахувати точні цифро дуже важко.

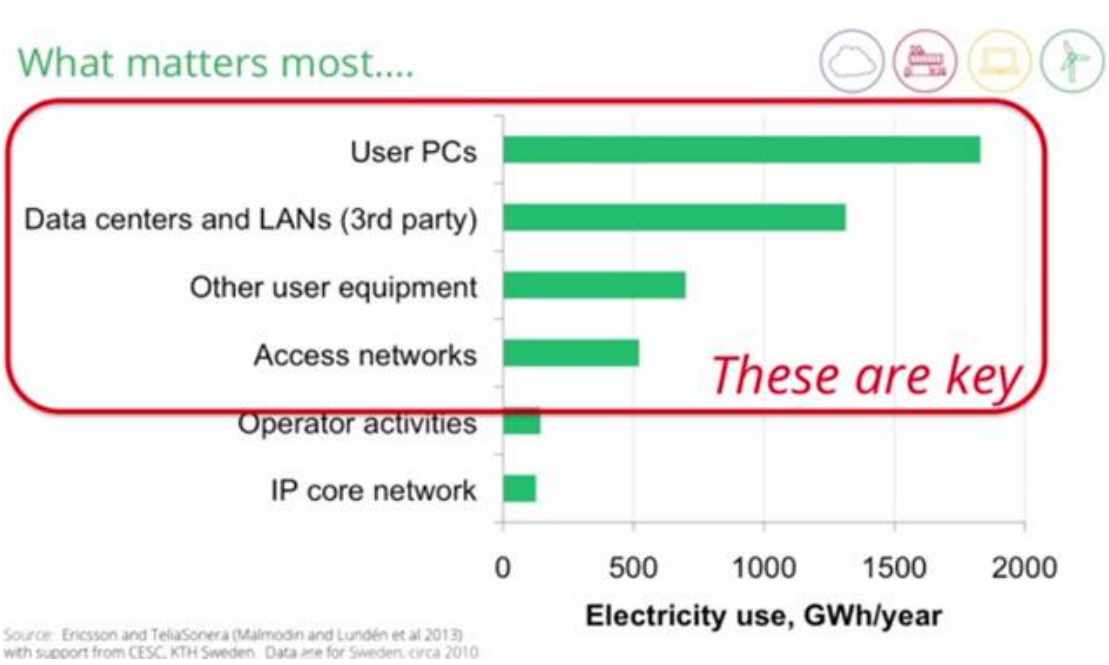

Рис.4.1. Чинники впливу на навколишнє середовище

На відміну від автомобіля, який виділяє паливо через вихлопну трубу, важко уявити вплив мережі на навколишнє середовище. Її вуглецевий слід в основному є результатом потужності, необхідної для підтримання роботи інфраструктури. Антени мобільних телефонів, пристрої, якими люди користуються для доступу до Інтернету, а також центри обробки даних вимагають величезної кількості електроенергії. Ця електроенергія може надходити з відновлюваних джерел, але часто це не відбувається. Наприклад, у своєму звіті «Наскільки чистою є ваша хмара?» Грінпіс виявив, що 70% від 400 000 антен мобільного телефону в Індії не мають доступу до надійних джерел електроенергії, а дизельні генератори використовуються для компенсації неадекватного енергопостачання. Великі центри обробки даних у західних країнах також покладаються на резервні дизельні генератори, які спрацьовують у разі відключення електроенергії [27].

4.1.1. Вплив центрів обробки даних

Центри обробки даних – це другий за енергоємністю елемент Інтернету після пристроїв. Центр обробки даних Facebook в Приневіллі, штат Орегон, споживає близько 78 мегават електроенергії, що дорівнює приблизно 64 000 будинкам.

Проте центри обробки даних є найефективнішим способом підтримання роботи Інтернету, враховуючи, що централізація серверів в одному місці дозволяє використовувати синергію та мінімізувати використання електроенергії. Однією з переваг хмари є те, що вона забезпечує набагато більшу концентрацію обчислювальної та обробної потужності при меншій кількості серверів, що завжди означає енергозбереження. Але єдиним способом зменшити забруднення є використання відновлюваних джерел енергії, а також підвищення енергоефективності [27-29].

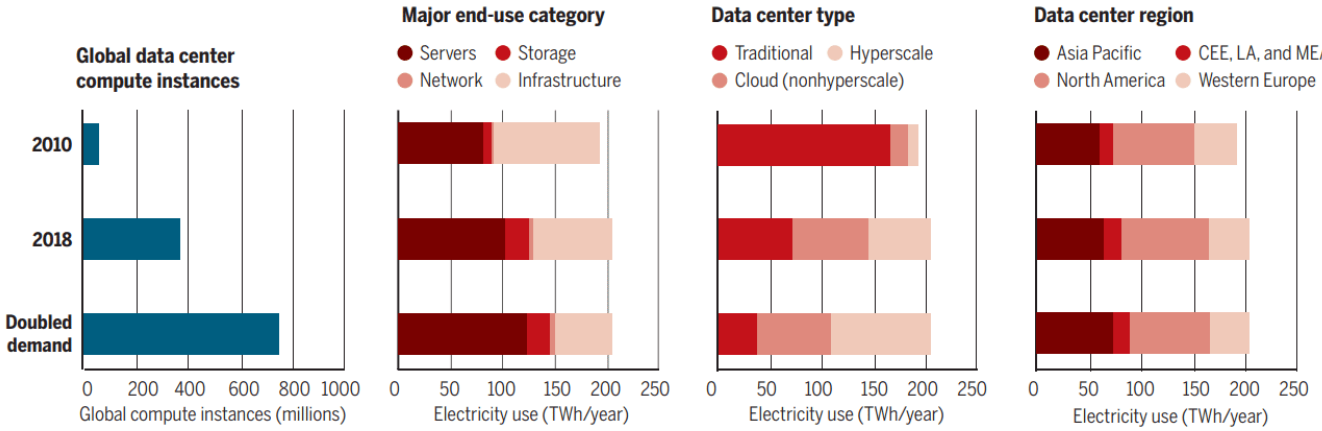

Рис.4.2. Історичне споживання енергії ЦОД в 2010-2018 рр і прогноз на найближчі роки, коли відбудеться чергове подвоєння кількості обчислювальних інстанси (ядер) в дата-центрах

Проблема пов'язана з джерелами енергії, які підтримують роботу центрів обробки даних. В даний час більшість центрів обробки даних працюють з енергетичними компаніями, які покладаються на вугілля або атомні електростанції для виробництва електроенергії.

В звіті «Наскільки чистою є ваша хмара?» встановлено, що 55,1% електроенергії, що використовується серверами Apple, виробляється вугільними заводами, 49,7% енергії, яку використовують сервери IBM, і 39,4% сервери Facebook. Ці значні цифри спричиняють тисячі тонн вуглекислого газу, що викидається в атмосферу та брудне повітря, яке з нею йде.

З 2000 по 2006 рік загальний інтернет-трафік зріс на 32 000 000%, тоді як загальне споживання енергії зросло лише на 200% за той самий період.

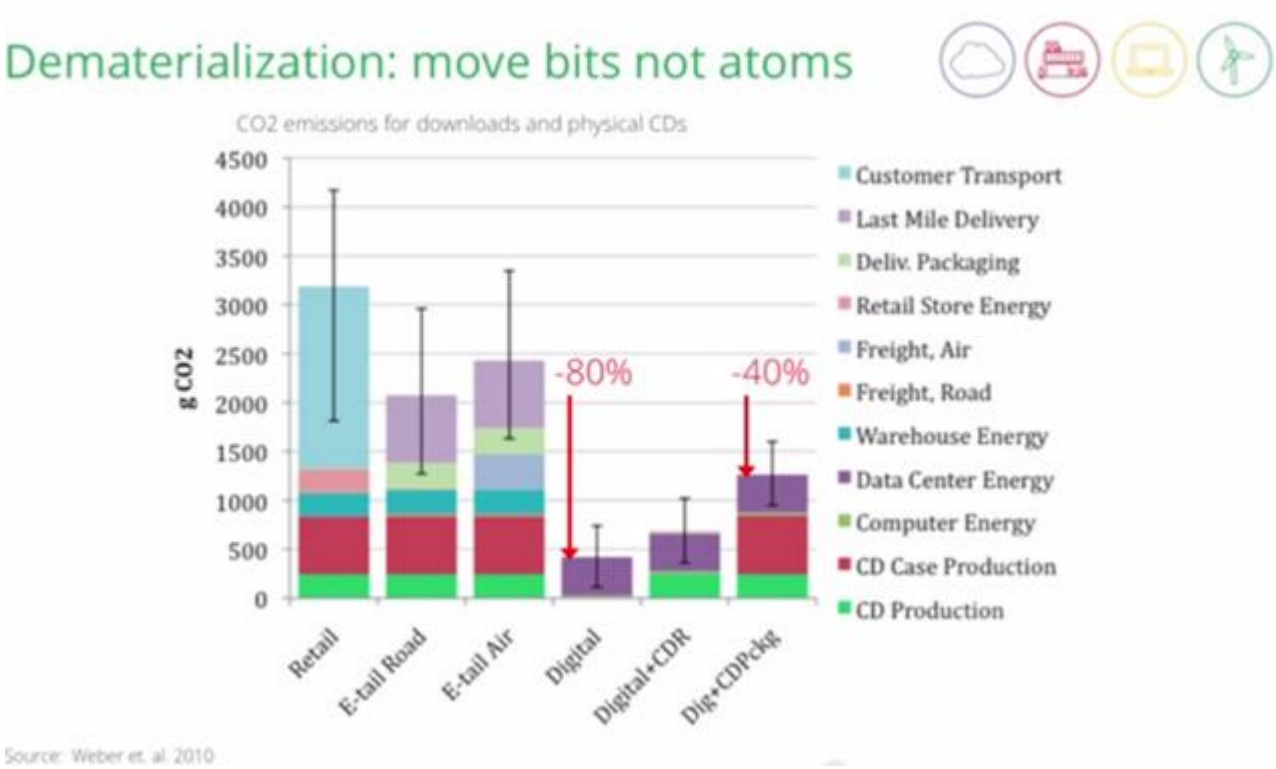

Рис.4.3. Чинники що впливають на викиди вуглекислого газу

В [30] автори інтегрували дані з різних джерел, які з'явилися останнім часом. Стаття написана декількома провідними експертами по використанню енергії в центрів обробки даних з Північно-Західного університету, Національної лабораторії Лоуренса Берклі і дослідницької компанії Koomey Analytics (США).

Новий аналіз показує досить скромне зростання енергоспоживання в останні роки. Зокрема, до 2018 року робочі навантаження і кількість обчислювальних інстансів збільшилася більш ніж в шість разів, IP-трафік збільшився більш ніж в 10 разів. Ємність сховищ ЦОД за цей термін виросла в 25 разів. Але з 2010 року споживання електроенергії в розрахунку на один сервер знизилося в чотири рази, в основному, завдяки технологічним поліпшеням і скороченню часу холостої роботи.

Показник ват на терабайт встановленої пам'яті знизився приблизно в дев'ять разів через збільшення щільності та ефективності накопичувачів.

Крім того, зростання числа серверів значно сповільнилося внаслідок п'ятикратного збільшення середнього числа інстанси на одному сервері (внаслідок віртуалізації).

При цьому протягом 2010-2019 років спостерігалося стійке поліпшення якості енерговитрат PUE (power usage effectiveness), яке обчислюється як частка від ділення загального енергоспоживання дата-центру на енергоспоживання його IT-обладнання. Внесок різних складових в змінах PUE показаний на діаграмі нижче.

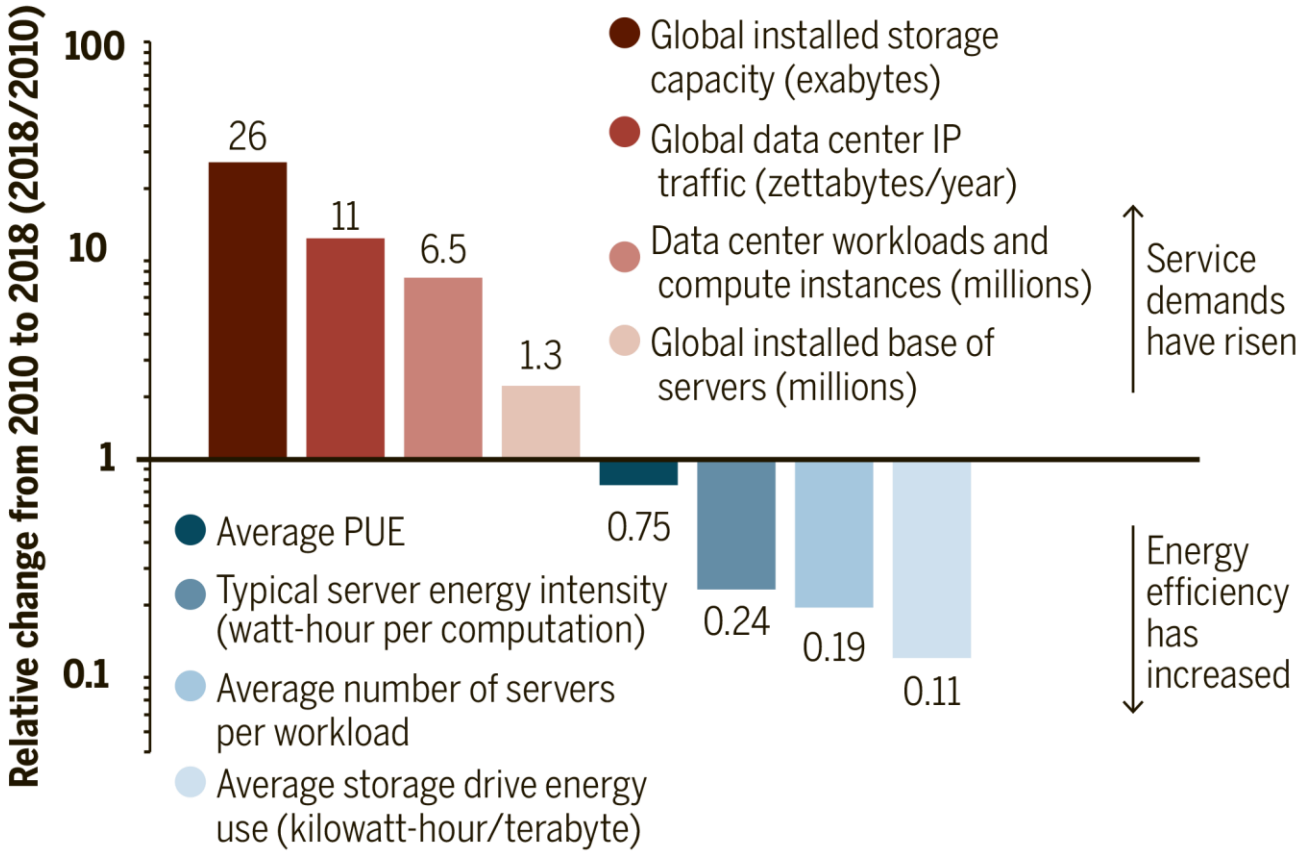

Рис.4.4. Тенденції в енергоспоживанні дата-центрів

У 2018 році глобальне споживання енергії дата-центрів зросло до 205 ТВт/год, що представляє собою збільшення всього на 6% в порівнянні з 2010 роком, тоді як загальна кількість «обчислювальних інстансів» збільшилася на 550% за той же період часу (під обчислювальними інстнасами маються на увазі обчислювальні ядра CPU, в першу чергу).

Якщо обчислити використання енергії на обчислювальний інстанси, то енергоємність кількість глобальних центрів обробки даних з 2010 року щорічно зменшувалася на 20%.

Загальне енергоспоживання дата-центрів у 2010-2018 роки практично не змінилося, зате енергоспоживання IT-пристроїв (серверів, систем зберігання та мережевого обладнання) зросла з 92 до 130 ТВт/ год, що вказує на збільшення ефективності ЦОД. Іншими словами, тепер більше енергії йде безпосередньо на роботу серверів, а менше - на допоміжні системи на зразок системи охолодження. У той же час це говорить про підвищення технологічної та експлуатаційної ефективності інфраструктури: «Це зниження пояснюється продовженням переходу від невеликих традиційних центрів обробки даних (79% обчислювальних інстанси в 2010) до великих і більш енергоефективним хмарним (включаючи гіпермасштабуємі) дата-центри (89% обчислювальних операцій в 2018 році)».

В найближчій перспективі ринкові аналітики прогнозують ще більшу віртуалізацію серверів, а технологічні дослідження вказують, що у IT-пристроїв зберігся потенціал для підвищення енергоефективності, в тому числі більше переходів на малопотужні пристрої.

З точки зору інфраструктури, надвеликі ЦОД світового класу вже працюють на PUE = 1,1 або нижче, що близько до мінімального можливого значення.

Дослідники прогнозують, що в короткостроковій перспективі продовжиться перехід від менших традиційних дата-центрів на більш ефективні гіпермасштабуємі ЦОД. При цьому є достатній ресурс енергоефективності для поглинання наступного подвоєння обчислювальних операцій в дата-центрах паралельно з незначним збільшенням обсягу глобального використання енергії.

Як приклад: PUE 1,95 означає, що на системи кондиціонування, охолодження та інші «комунальні» потреби Цода використовується 95% енергії щодо потреби серверів в ЦОД.

У більшості дата-центрів Китаю PUE дорівнює 2,2. Це набагато вище, ніж в ряді європейських країн. А в США середній PUE дорівнює 1,9. Компанії-лідери за показником демонструють цифру не більше 1,2.

4.1.2. Реалізації ЦОД міжнародних корпорацій

У питанні успішного поєднання екологічної відповідальності та інновацій особливо виділяється невелика, але дуже технологічне держава - Сінгапур. Google, Amazon і IBM вже розмістили тут свої серверні «ферми». Країна може похвалитися високою концентрацією дата-центрів з надшвидким підключенням і за рахунок цього йде в ногу з поколінням високих технологій, забезпечуючи благодатний грунт для розвитку віртуалізації і мобільності.

Сінгапунські інженери Tropical Data Center (TDC) провели експеримент зі створенням першої в світі серверної «ферми» для умов тропічного клімату. Мета – дослідити можливості для застосування екологічно чистих технологій в дата-центрах. А глобальна ідея - знизити енергоспоживання інфраструктури серверних ферм. Сінгапур - це саме та країна, про яку ми говорили вище: 7% з загального споживання електроенергії йде в раціон сінгапурських Цодов.

Багато IT-компанії і навіть технологічний університет вирішили взяти участь в експерименті, надавши свої ресурси і розробки. У його рамках буде проводитися перевірка серверів на витривалість при скачках напруги, відсутності температурного контролю або контролю вологості.

Apple заслуговує звання екологічно відповідальної корпорації, реалізувавши безліч еко-проектів, незважаючи на те, що деякий час відчувала тиск з боку захисників екології. Зараз в Каліфорнії офіс Apple Park має на даху найпотужнішу сонячну установку, компанія щосили встановлює масиви сонячних батарей на полях Невади, Каліфорнії і Китаю.

iDataCenter у Apple зовні він пофарбований у білий колір - для зменшення нагрівання сонцем; в ЦОДі трифазне електропостачання обладнання; у всій будівлі використовуються енергозберігаючі LED-світильники. За подібну «дружність» до навколишнього середовища iDataCenter був відзначений сертифікатом LEED Platinum .

Інше джерело енергії для iDataCenter - станції, що працюють на біогазі. Газ отримують від розкладання біомаси. Вироблений станціями метан проходить очист-

ку і акумулюється в паливних елементах Bloom Box, які потім постачають електроенергією сервери компанії.

Плюсів такої моделі багато: по-перше, це безвідходний спосіб отримання електроенергії, а по-друге, надлишок тепла, що виділяється прямує назад в переробну камеру для прискорення процесу бродіння. А метан є поновлюваним і досить доступним ресурсом.

Microsoft в 2013 році відмовився від підключення до регіональної енергетичної інфраструктури. Дата-центр став сам собі енергокомпанією. Microsoft впровадив метанові паливні елементи прямо в серверні стійки. Впровадження автономного джерела живлення в інфраструктуру ЦОД дозволило оптимізувати розподіл енергії. Ефективність дата-центру зросла вдвічі. Такий ЦОД можна розмістити всюди, де є метан у видаленні від інфраструктури міста.

Ключову роль в майбутньому при розгортанні обчислювальної інфраструктури Microsoft можуть зіграти підводні ЦОДи Project Natick. Коли компанія запустила цей проект, всі навколо сприймали його як експеримент. Але зараз Microsoft інтегрував концепцію підводних ЦОД в свою стратегію «крайових обчислень», яка передбачає максимальну близькість даних до кінцевих користувачів. Підводний дата-центр є автономним і працює від відновлюваної енергії.

У Facebook ефективність використання електроенергії дата-центром (PUE) в Лулео становить всього 1,07. Цей регіон знаходиться в 60 кілометрах від Полярного кола. Facebook використовує в ЦОДі тільки енергію, одержувану з гідроелектростанції в місці впадання річки Лулі в Ботнічна затока. Середня температура тут - всього 1°C. Компанії вдалося знизити кількість запасних генераторів на 70%.

Розробники з DeepMind, дочірньої компанії Google, створили інтелектуальну модель контролю ефективності споживання енергії на базі штучного інтелекту DeepMind. Система працює за принципом кількісного виміру задіяного обладнання в різний час: кондиціонери, системи відкриття/закриття вікон, швидкість роботи вентиляторів, насосів, контроль температури, споживання енергії, активності чиллерів і т.п.

Також компанія до 2018 року вже повністю перевела електропостачання своїх ЦОД на поновлювані джерела енергії. Google поступається першістю енергоефективності лише Facebook - в її дата-центрі PUE досяг 1,12.

Інший ЦОД Google може приймати енергію вітру. Мета проекту - забезпечити плавучий дата-центр на вітряної енергії. Її будуть генерувати величезні повітряні змії високо над поверхнею води, де повітряні потоки перманентні. Змії-генератори будуть ще й приводити суду в рух - прямо як вітрила.

Цей нідерландський ЦОД Equinix AM3 знаходиться в Амстердамі. Його оператор використовує гібридні охолоджувальні вежі Aquifer Thermal Energy Storage. Прохолодне повітря веж використовується для зниження температури гарячих коридорів. Вода відводить тепло від серверів і стійок, нагрівається і тут же відправляється в систему опалення Амстердамського університету. Для особистих потреб амстердамський ЦОД генерує близько 800 тисяч кіловат-годин на рік.

На початку вересня 2019 року Британська енергетична компанія Simec Atlantis Energy оголосила про будівництво в Шотландії дата-центру, який буде працювати виключно від поновлюваного джерела енергії. Електрика надходитиме від гідроелектростанції, що використовує енергію припливів. Це перший дата-центр в світі, що працює від такого роду джерела енергії. А його вдале розташування в перешийку між берегом Шотландії і островом Строма дозволить станції економити на системі охолодження і отримувати енергію за рахунок руху потоків величезних обсягів вод. Протікаючи між берегами, вода буде розкручувати турбіни станції і забезпечувати ЦОД екологічно чистою електроенергією.

4.3. Вплив споживання електроенергії на людину та її оточення

Споживання енергії притаманне майже всім видам господарської діяльності людини, а саме - опалення будинків, приготування їжі, руху транспортних засобів, промисловості, сільськогосподарського виробництва і т.д. Освоєння різних видів енергії в світовому масштабі призвело до безпрецедентного зростання рівня життя.

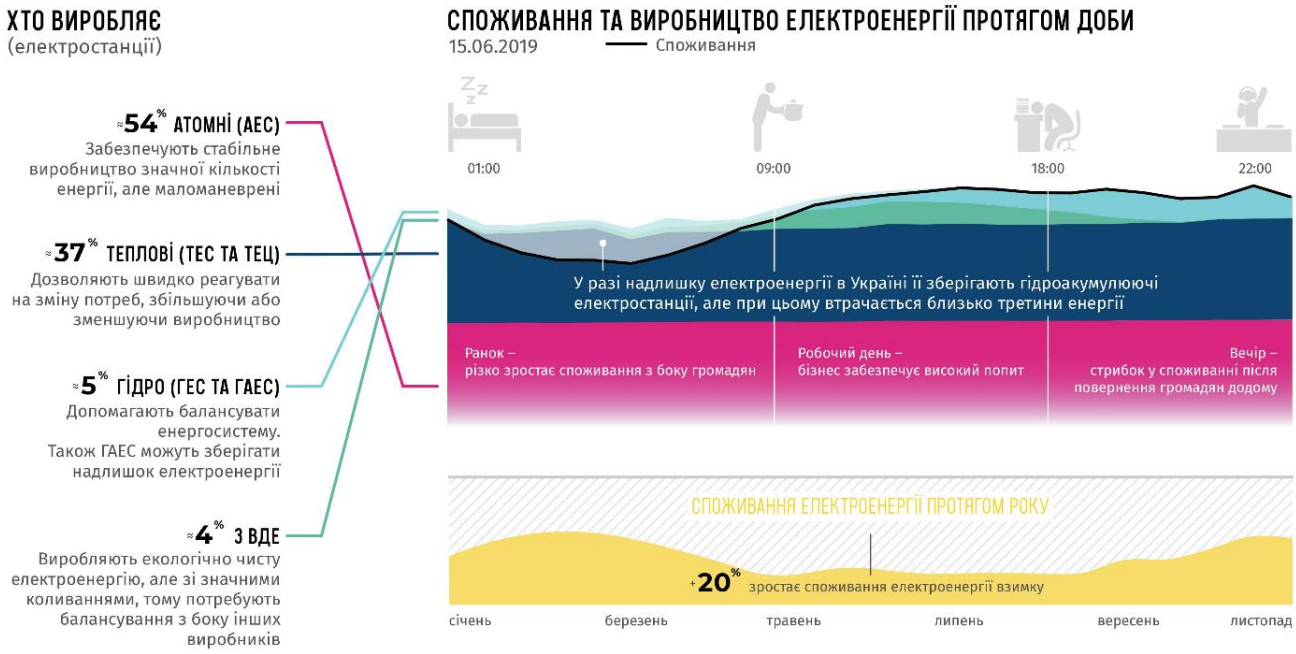

Рис.4.5. Виробництво та споживання електроенергії в Україні

Основні джерела енергії, доступні зараз людині, можна класифікувати наступним чином:

- викопне паливо (вугілля і горючі сланці, нафта, природний газ);
- ядерна та термоядерна енергія;
- поновлювані енергетичні ресурси (енергія води, вітру, сонця, термальних вод, деревини, торфу і т.д.).

Виробництво енергії істотно впливає на стан навколишнього середовища. Спалювання викопного твердого та рідкого палива супроводжується виділенням сірчистого, вуглекислого та чадного газів, а також оксидів азоту, пилу, сажі та інших забруднюючих речовин.

Видобуток вугілля відкритим способом і торфорозробки ведуть до зміни природних ландшафтів, а іноді - і до їх руйнування. Розливи нафти і нафтопродуктів при видобутку і транспортуванні здатні знищити все живе на величезних територіях (акваторіях).

Дуже погано позначається на ландшафтах, рослинному і тваринному світі створення інфраструктури, необхідної для вугле-, нафто- і газовидобутку.

Будівництво та експлуатація великих гідроелектростанцій призводить до: відселенню людей із зони затоплення, знищення цінних видів риб, для яких греблі стають нездоланними перешкодами на шляху до нерестовища, втрати лісів і високородючих земель, збільшення ризику виникнення руйнівних землетрусів в передгірних і гірських районах, підвищення ризику катастрофічних повеней в місцевостях, що знаходяться нижче за течією, зміни ландшафтів і їх руйнування.

Атомна енергетика є потенційно небезпечною через можливі аварії на енергоустановках, що супроводжуються викидом у навколишнє середовище радіоактивних матеріалів. Крім того, виникають проблеми переробки ядерних відходів і їх захоронення, що обходиться дуже дорого і не має надійного інженерного рішення. Ядерні відходи залишаються небезпечними протягом сотень і тисяч років. Особливо актуальна ця тема для України, яка постраждала від наслідків вибуху на Чорнобильській АЕС.

Незважаючи на очевидні переваги, поновлювані джерела енергії також можуть негативно впливати на навколишнє середовище. Експлуатація станцій, які виробляють енергію за допомогою поновлюваних енергетичних джерел, пов'язана з вилученням з обігу значних земельних ділянок і, ймовірно, в майбутньому буде супроводжуватися тими чи іншими негативними наслідками для навколишнього середовища: змінами ландшафтів (вітряки, сонячні батареї), підвищений рівень шуму (вітряки), забруднення грунтів (геотермальні енергоустановки і установки, що працюють на біомасі), згубними впливами на інші природні ресурси (припливно-відливних електростанції).

З огляду на вищеописану ситуацію, раціональним рішенням можна вважати енергозбереження. Саме воно має стати пріоритетним в стратегії розвитку будь-якої країни, адже запаси традиційних джерел енергії обмежені.

4.3. Рекомендації щодо зниження негативного вливу ЦОД

У 2016 році The Green Grid розробила й опублікувала глобальний стандарт коефіцієнта PUE для оцінки енергоефективності дата-центрів. Хоча PUE використовували і раніше, галузевим стандартом він став недавно.

PUE (Power Usage Effectiveness) – показує, наскільки ефективно ЦОД використовує енергію, яку отримують його споживачі. Коефіцієнт PUE регулярно включають в свої розрахунки найбільші власники центрів обробки даних, такі як Microsoft і Google.

PUE показує відношення сумарної потужності ЦОД до сумарної потужності повного набору IT-обладнання: серверів, систем зберігання даних, комутаторів та інших мережевих пристроїв.

$$POE = \frac{\text{сумарна потужність ЦОД}}{\text{сумарна потужність повного набору IT обладнання}}$$

При ідеальній організації ЦОД PUE не перевищує значення 1.25, а в оптимальному випадку знаходиться в межах 1.25-1.43 одиниць. Компанії, які не вживають заходів для підвищення енергоефективності, в розрахунках отримують більше 2.5 одиниць.

Приклади розрахунку PUE для центру обробки даних

1) ЦОД купує всю електроенергію

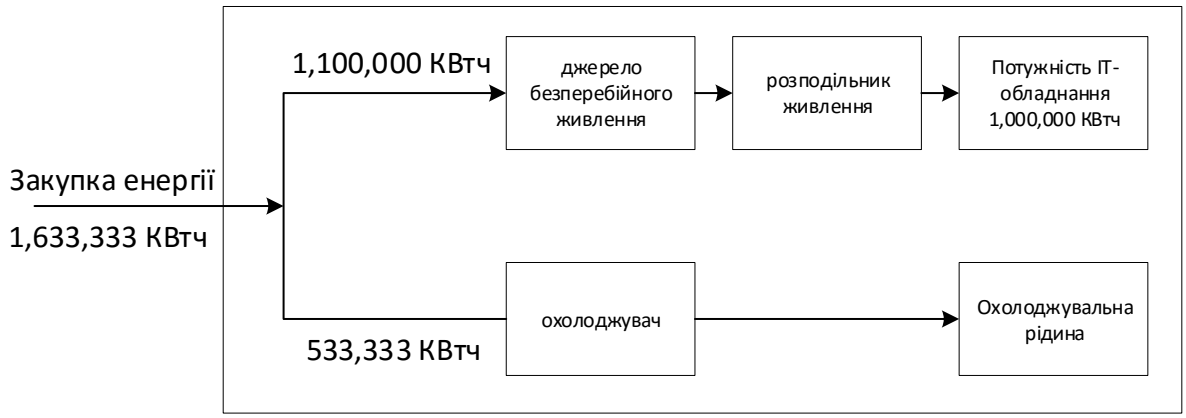

Рис.4.6. ЦОД купує всю електроенергію

$$PUE = \frac{1{,}633{,}333 * \mathbf{1}}{1{,}000{,}000 * \mathbf{1}} = 1.63$$

2) ЦОД купує електроенергію та охолоджувальну рідину

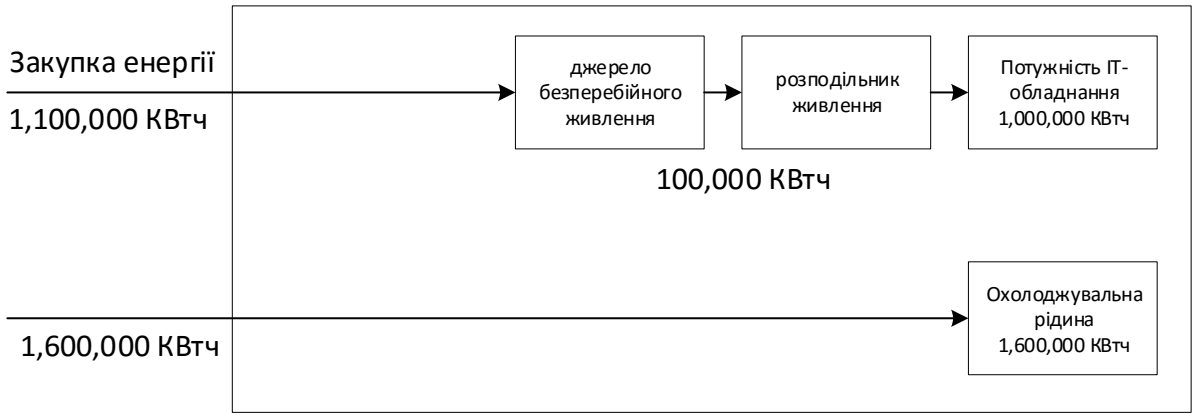

Рис.4.7. ЦОД купує електроенергію та охолоджувальну рідину

$$PUE = \frac{1{,}100{,}000 * 1 + 1{,}600{,}000 * 0.4}{1{,}000{,}000 * 1} = 1.58$$

Наступне рівняння ілюструє, як кількісно визначити використання енергії системи охолодження для центру обробки даних, яка має загальну установку охолоджувальної рідини.

$$Q = \frac{VHC * \text{швидкість потоку} * \Delta T * \text{час}}{\text{Перетворення енергії}}$$

де Q – енергія від тепла, захопленого охолодженою рідиною, в мегават-часах (МВтч)

VHC – об'ємна теплоємність, властивість текучого середовища, яке зазвичай використовується на установках з охолодженою водою.

$$VHC = \text{Щільність рідини} * \text{Специфічна теплота рідини}$$

Швидкість потоку – витрата охолодженої води (наприклад, кубічні метри на секунду (м3/с)

ΔT – різниця температур між подачею та поверненням охолодженої води (Кельвін)

Час – проміжок часу для вимірювання енергії (використовуючи ту саму часову базу, що і знаменник витрати)

Перетворення енергії – стандартне перетворення, необхідне для зміни одиниць вимірювання енергії з Джоулів на МВтч.

Приклад розрахунку:

$$VHC = 1{,}000\,^{kg}/_{m^3} * 4.184\,^{J}/_{(kg * °K)} = 4.184.000\,^{J}/_{(m^3 * °K)}$$

Швидкість потоку $= 0{,}003\,^{m^3}/_{s}$

$\Delta T = 5°C = 5°K$

Час = 1 рік = 31,536,000 s

Перетворення енергії = $3{,}600{,}000{,}000\,^{J}/_{MWh}$

$$Q = \frac{4.184.000\,^{J}/_{(m^3 * °K)} * 0{,}003\,^{m^3}/_{s} * 5°K * 31{,}536{,}000\ s}{3{,}600{,}000{,}000\,^{J}/_{MWh}} = 549{,}78 MWh$$

Щоб знизити PUE можна імплементувати природнє охолодження, моніторинг і прогнозоване обслуговування, зменшувати фізичні сервери та збельшувати кількість віртуальних машин.

Близько 40% всієї енергії, яку споживають дата-центри, йде на роботу штучних систем охолодження. Істотно знизити витрати допомагає реалізація природного охолодження (фрікулінга). При такій системі зовнішнє повітря фільтрується, підігрівається або охолоджується, після чого подається в серверні приміщення. «Відпрацьоване» гаряче повітря викидається назовні або частково підмішується при необхідності до вхідного потоку.

У разі фрікулінга велике значення має клімат. Чим більше температура повітря на вулиці підходить для залу дата-центру, тим менше потрібно енергії, щоб доводити його до потрібної «кондиції».

Крім того, дата-центр може розміщуватися у водоймах, в такому випадку вода з нього може використовувати для охолодження ЦОД. За прогнозами Statistics MRC, до 2023 року вартість ринку технологій рідинного охолодження досягне $4.55 млрд. Серед його видів виділяють іммерсійне охолодження (занурення обладнання в іммерсійне масло), адіабатичне охолодження (в основі - технологія випаровування, використовується в ЦОД Facebook) , теплообмінне (теплоносій потрібної температури надходить безпосередньо до стійки з обладнанням, видаляючи надлишки тепла).

Підвищити енергоефективність також допоможе правильне використання потужностей, якими володіє дата-центр. Вже придбані сервери повинні або працювати на завдання клієнтів, або не споживати енергію під час простою. Один із способів контролювати ситуацію - використовувати ПЗ для керування інфраструктурою. Наприклад, систему Data Center Infrastructure Management (DCIM). Таке ПЗ автоматично перерозподіляє навантаження на сервери, відключає незадіяні пристрої і дає рекомендації по швидкості роботи вентиляторів холодильних установок (знову ж таки, для економії енергії на зайвому охолодженні).

Важлива частина підвищення енергоефективності ЦОД - своєчасне оновлення обладнання. Застарілий сервер найчастіше поступається по продуктивності і ресурсоємності новому поколінню. Тому для зниження PUE рекомендовано оновлювати обладнання якомога частіше - деякі компанії роблять це щороку. З дослідження Supermicro: оптимізовані цикли оновлення обладнання дозволять скоротити обсяг електронних відходів більш ніж на 80% і підвищити продуктивність ЦОД на 15%.

Існують також способи оптимізації екосистеми дата-центрів без істотних витрат. Так, можна закрити щілини в серверних шафах, щоб запобігти витоку холодного повітря, ізолювати гарячий або холодний коридори, перенести високонавантажених сервер в більш холодну частину ЦОД і так далі.

Компанія VMware підрахувала, що перехід на віртуальні сервери в ряді випадків знижує електроспоживання на 80%. Це пояснюється тим, що розміщення більшої кількості віртуальних серверів на меншій кількості фізичних машин логічно скорочує витрати на обслуговування «заліза», охолодження і харчування.

Експеримент компаній NRDC і Anthesis показав, що заміна 3 000 серверів на 150 віртуальних машин економить $ 2 млн на електриці.

Крім іншого, віртуалізація дає можливість перерозподіляти і нарощувати віртуальні ресурси (процесори, пам'ять, обсяг сховища) в процесі. Тому електроенергія витрачається тільки на забезпечення роботи, виключаючи витрати на обладнання, що простоює.

Безумовно, для підвищення енергоефективності можна також вибирати альтернативні джерела енергії. Для цього деякі ЦОД використовують сонячні батареї і вітряні генератори. Це, однак, досить дорогі проекти, які можуть собі дозволити тільки великі компанії..

4.4. Висновки до розділу 4

Проведено аналіз впливу інформаційних технологій, зокрема центрів обробки даних, на навколишнє середовище. В результаті встановлено, що в найближчі роки швидкого зростання споживання електроенергії центрами обробки даних не передбачається. Але обсяг обчислень буде рости безперервно ще багато десятиліть, так що енергоспоживання в ЦОД необхідно контролювати. Рекомендується стежити за дотриманням стандартів, таких як Energy Star, для серверів, сховищ і мережевих пристроїв, вимагати такої сертифікації для державних закупівель. Виробникам обладнання потрібно створити стимули для продовження випуску інноваційних енергоефективних продуктів.

РОЗДІЛ 5 Охорона праці

5.1. Аналіз шкідливих та небезпечних факторів при експлуатації «Системи контролю доступом»

Робота з налаштуванням системи ведеться в приміщенні 7 м на 5 м, висота приміщення 2,5 м: площа приміщення становить 35 метрів квадратних, а об'єм - 87,5 метрів кубічних. Кількість робочих місць - 2. Система опалення централізованого типу, складається з двох батарей. Наявне природне і штучне освітлення комбінованого типу: природне освітлення - вікно 2 на 2 метри; штучне освітлення представлене світильником загального освітлення і настільною лампою на робочому місці.

При роботі з системою на інженера-програміста можуть діяти наступні небезпечні та шкідливі виробничі фактори відповідно [ГОСТ-12.0.003-74, [31]:

- знижена температура повітря робочої зони;
- нестача природного світла;
- недостатня освітленість робочої зони;
- розумове перенапруження;
- емоційні перевантаження.

Знижена температура повітря робочої зони

Допустимі величини температури, відносної вологості та швидкості руху повітря в робочій зоні виробничих приміщень

Період року	Категорія робіт	Температура, град. С			
		Верхня межа		Нижня межа	
		На постійних робочих місцях	На непостійних робочих місцях	На постійних робочих місцях	На непостійних робочих місцях
Холодний період року	Легка Іб	24	25	20	17

Теплий період року	Легка Іб	28	30	21	19

Робота інженера-програміста відноситься до категорії Іб, а отже температура повітря повинна відповідати 20-24 гр. С в холодний період року, а в теплий період – 21-28 гр. С.

Температура повітря в січні місяці (гр. С)

Фактичне значення: 19 ГДР: 20-24

Нестача природнього світла (КПО, %):

Фактичне значення: 1 ГДР: 1,5

Недостатня освітленість робочої зони

Фактичне значення: 180-220 лк ГДР: 300 лк

Розумове перенапруження (годин безперервної роботи):

Фактичне значення: 2 ГДР: 1

Емоційне перевантаження

Шкідливі рівні (напружена праця):

1 ступінь	Несе відповідальність за функціональну якість основної роботи (завдань). Вимагає виправлень за рахунок додаткових зусиль всього колективу (групи, бригади та ін.);
2 ступінь	Несе відповідальність за функціональну якість кінцевої продукції, роботи, завдання. Неправильні рішення можуть викликати пошкодження обладнання, зупинку технологічного процесу, можливу небезпеку для життя.

Емоційні перевантаження 2 ступеня шкідливого рівня (напружена праця)

5.2. Розрахунок та розробка інженерно-технічних заходів з охорони праці при розробці системи контролю доступу

Знижена температура повітря робочої зони

Для забезпечення оптимальних значень параметрів необхідно кондиціонування повітря. Відповідно до норм оптимальні умови створюються там, де це передбачено галузевими документами. В інших виробничих приміщеннях мають забезпечуватися допустимі метеоумови (табл.).

Таблиця. Межі зміни параметрів метеоумов у виробничих приміщеннях

Параметр	Значення параметрів	
	оптимальні	допустимі
Температура повітря, °С	16-25	13-29
Відносна вологість, %	60-40	До 75
Швидкість руху повітря, м/с	0,1-0,4	0,1-0,6

У виробничих приміщеннях, де з технічних чи економічних причин неможливо забезпечити допустимі нормативні показники мікроклімату, мають передбачатися заходи щодо захисту працюючих від перегрівання чи охолодження.

Нестача природного світла

Враховуючи те, що найбільш небезпечним прийнятий чинник нестачі освітлення, розглянемо його детальніше. Для збільшення КПО будемо впливати на коефіцієнт, що враховує підвищення КПО завдяки світлу, яке відбивається від поверхонь приміщення. Виключаємо можливість зміни площі вікна через архітектурну недоцільність.

I) Мінімально необхідний КПО становить 1.5% [СНиП-23-05-95, [32]. Використаємо перевірочний метод, для визначення реального стану природної освітленості приміщення за формулою(1):

(1)

Враховуючи, що площа підлоги становить 35 метрів квадратних, а площа вікна - 4 метри квадратних, отримаємо:

$$\alpha = \frac{4}{35} \times 100\% = 11\%$$

КПО рівне 1.5% відповідає середньому класу точності (IV), а мінімальній коефіцієнт α для такого класу робіт - не менше 12% [ДСанПіН-3.3.2-007-98, [33]. Для підвищення ефективності освітлення робочої поверхні варто прийняти такі заходи:

- Розмістити робочу поверхню на відстані 1 м навпроти вікна так, щоб вікно, відносно робочої поверхні було ліворуч.

- Використати фарбу або шпалери для стін, тип покриття підлоги та стелі так, що матимуть більший коефіцієнт відбиття світла.

Розрахуємо КПО за нових умов за формулою(2):

Де $K_з$ — коефіцієнт запасу; ηВ —світлова характеристика вікон; — коефіцієнт, що враховує затінення вікон будівлями, розташованими навпроти; — загальний коефіцієнт світлопропускання світлових прорізів; r_1 — коефіцієнт, що враховує підвищення КПО завдяки світлу, яке відбивається від поверхонь приміщення

1) $K_з$ для приміщення з нормальними умовами середовища становить 1,2. визначається таблично із співвідношення довжини приміщення до глибини і глибини до відстані робочої поверхні до краю вікна: Для нашого випадку ці співвідношення становлять: 0,7 та 3,5. Отже ηВ = 18 виходячи з табличних даних.

3) Будівлі навпроти значно нижче за поверх, на якому знаходиться приміщення, а отже приймемо

4) r_1 визначається залежно від характеристик поверхонь в середині приміщення та відстані робочої поверхні до вікна. Саме на цей коефіцієнт необхідно вплинути, щоб збільшити КПО і підвищити його за ГДР.

Ключовими співвідношеннями є відношення відстані від робочої поверхні до вікна порівняно з глибиною приміщення, так середнє значення відбиття світла пове-

рхнями в кімнаті . Відстань до вікна ми визначили рівною 1 метру, а отже перше співвідношення буде рівне 1/7. розраховується за формулою (3):

(3)

Ми не можемо змінити геометричні розміри кімнати, проте можемо визначити тип поверхонь. Приймемо такі значення:

Стеля: Свіже побілена

Стіни: Свіже побілені із жалюзі = 0,60

Підлога: Біла, матова плитка = 0,82

Кінцевий результат:

Розрахунок проведено за рекомендацією [СНиП-23-05-95, [32] (без урахування сторонніх об'єктів).

r_1 визначаємо за таблицею по отриманим значенням и отримуємо: $r_1 = 7{,}2$

5) визначається за формулою(4):

(4)

де, τ_1 — коефіцієнт світлопропускання матеріалу вікон

τ_2 — коефіцієнт, що враховує втрати світла у віконній рамі

τ_3 — коефіцієнт, що враховує втрати світла у сонцезахисних пристроях

Коефіцієнти - табличні данні, що залежать від типу вікна:

1) Скло листове подвійне $\tau_1 = 0{,}8$

2) Рама металева подвійна і відкривається $\tau_2 = 0{,}8$

3) Присутні горизонтальні жалюзі $\tau_3 = 0{,}7$

Підставимо отримані данні в формулу (5):

$$КПО = \frac{4 \times 0{,}45 \times 7{,}2 \times 100}{1{,}2 \times 18 \times 1 \times 35} = \frac{1296}{760{,}2} = 1{,}7\%$$

При виконанні вищезазначених умов можна усунути проблему нестачі природного освітлення і забезпечити умови для виконання робіт класу IV.

Недостатнє освітлення робочої зони

Для роботи, пов'язаної зі сприйняттям інформації з екрана [СП-12.13130.2009, [34], спосіб освітлення всього приміщення не є достатнім. При необхідності реєстрації та сприйняття інформації з екрану, яскравість робочого місця, створювана місцевим освітленням, де відбувається ця реєстрація, повинна відповідати яскравості екрана (75–100 кд/м2), при чому екран має бути захищеним від прямого влучення променів світла.

Розумове перенапруження

Правилами встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці: для операторів із застосуванням ЕОМ слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години.

Для запобігання розумового перенапруження рекомендовано кожну годину роботи робити перерву на 15 хвилин для попередження нервових зривів.

Емоційне навантаження

Аби знизити ступінь відповідальності за результат своєї діяльності необхідно аби наукового співробітника ніс відповідальність не за функціональну якість допоміжних робіт, а за виконання окремих елементів завдання, тобто «перенести» з середнього ступеня напруженості праці у легкий ступінь

Профілактика емоційного навантаження включає в себе регулярний відпочинок, вихідні на природі, тарифна відпустка, подорожі, заняття спортом, танці, психологічний аутотренінг, йогу, тімбілдінг. Психологи радять навчитись досягати і цінувати результат, замінити почуття провини на відповідальність, тобто якщо винен – не займайся самоїдством, а виправ по можливості, що можеш.

5.3. Пожежна безпека приміщення

Приміщення з повинні бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог «Переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з розрахунку 2 шт. на кожні 20 кв. м площі приміщення з урахуван-

ням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог Правил пожежної безпеки в Україні».

Приміщення, в якому розробляється макет, відноситься до категорій приміщень типу Д "Знижена пожежна небезпечність" (відсутні матеріали, що легко займаються) і має II клас вогнестійкості (стіни та перекриття - бетонні) [СП-12.13130.2009, [34].

Потенційну пожежну небезпеку становлять електромережа та ЕОМ: коротке замикання може спричинити суттєве нагрівання структурних елементів ЕОМ і спричинити їх займання.

Для запобігання займання, поряд з розетками електромережі, блоків живлення та силових контактів не повинні лежати жодні предмети, що можуть проводити струм та спричинити коротке замикання, або які є пожежонебезпечними.

Заборонено:

- експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією; залишення під напругою кабелів та проводів з неізольованими провідниками;
- застосування саморобних продовжувачів, які не відповідають вимогам до переносних електропроводок;
- застосування для опалення приміщення нестандартного (саморобного) електронагрівального обладнання або ламп розжарювання;
- користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;
- підвішування світильників безпосередньо на струмопровідних проводах, обгортання електроламп і світильників папером, тканиною та іншими горючими матеріалами, експлуатація їх зі знятими ковпаками (розсіювачами);
- використання електроапаратури та приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів.

Осіб, які не пройшли інструктаж з пожежної безпеки, не можна допускати до роботи. Кожен працівник зобов'язаний виконувати вимоги щодо пожежної безпеки, а також вживати заходів щодо усунення порушень правил пожежної безпеки, ліквідації пожеж і загорянь. Кожен працівник повинен знати місце розташування первинних засобів пожежогасіння і вміти ними користуватися, працівники повинні знати правила поведінки при пожежі, шляхи евакуації. У разі виникнення пожежі працівники повинні негайно повідомити про це пожежну охорону (по телефону) та керівництво установи і розпочати ліквідацію пожежі всіма наявними засобами.

У разі виявлення запаху горілого, диму або іскор негайно вимкнути напругу на щитку і візуально перевірити чи не виникло займання. У разі займання - сповістити оточуючих про наявність пожежі та докласти можливих зусиль для її локалізації.

5.4. Інструкція з охорони праці при роботі з «Системою контролю доступу»

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 До роботи допускаються Працівники, що пройшли:

- Професійну підготовку на підприємстві;
- Медичний огляд;
- Вступний інструктаж;
- Спеціальне навчання і перевірку знань з охорони праці;
- Первинний інструктаж на робочому місці.

1.2 Перевірка знань з охорони праці проводиться раз на 12 місяців в обсязі інструкцій з охорони праці.

1.3 Інструкція має переглядатись не рідше одного разу на 3 роки.

1.4 Професія інженера-конструктора пов’язана з такими видами небезпеки:

- Ураження струмом;
- Запиленість приміщення;
- Тривалий вплив штучного світлового випромінювання.

2. ВИМОГИ БЕЗПЕКИ ПЕРЕД ПОЧАТКОМ РОБОТИ

2.1 За 10 хвилин до початку роботи Працівник має прибути на робоче місце і підготувати його до роботи.

2.2 Працівник має оглянути робочий стіл, протерти його, перевірити правильність підключення електроприладів.

2.3 Працівник має ввімкнути основні електроприлади і освітлення.

2.4 Працівник має розкласти необхідні для роботи інструменти на столі. Інші предмети, не призначені для роботи не мають знаходитися на робочому місці під час робочого дня.

2.5 У разі виявлення проблем, Працівник має повідомити безпосереднього начальника.

3. ВИМОГИ БЕЗПЕКИ ПІД ЧАС РОБОТИ

3.1 Під час роботи з електронними приборами, Працівник має керуватися правилами електробезпеки: не торкатися оголених провідників струму; при роботі з чутливою електронікою користуватись заземленням; не відключати обладнання від мережі, якщо воно ще працює і не вимкнене; не залишати ввімкненими електроприлади, якщо необхідно покинути робоче місце з важливої причини.

3.2 Якщо під час роботи виявлено наявність забруднення від робочого процесу, яке заважає подальшій роботі, то таке забруднення має бути прибране тим Працівником, що його спричинив, в найближчий термін.

3.3 Якщо природного освітлення достатньо для роботи, Працівник може вимкнути штучне освітлення свого робочого місці, для зниження навантаження на очі.

3.4 Працівник не має відволікати інших Працівників під час роботи.

3.5 У разі виявлення порушень, Працівник має повідомити безпосереднього начальника.

4. ВИМОГИ БЕЗПЕКИ ПІСЛЯ ЗАКІНЧЕННЯ РОБОТИ

4.1 Після завершення робочого дня, Працівник має відкласти незавершені проекти у спеціально призначений для цього відділ робочого місця; зберегти результати роботи електроприладів, якщо це необхідно.

4.2 Працівник має вимкнути всі електричні прилади на робочому місці і перевірити їх стан.

4.3 Працівник має скласти інструменти до відповідних відділів робочого місця і перевірити, чи наявні всі інструменти, що були використані під час робочого дня і в якому вони стані.

4.4 При виявленні будь-яких проблем, Працівник зобов'язаний повідомити безпосереднього начальника.

5. ВИМОГИ БЕЗПЕКИ В АВАРІЙНИХ СИТУАЦІЯХ

5.1 При виникненні аварійної ситуації, Працівник має негайно припинити роботу і повідомити безпосереднього начальника про випадок.

5.2 При загорянні електропроводки або самих електроприладів, Працівник має знеструмити робоче місце, повідомити про випадок безпосереднього начальника та вжити заходів щодо локалізації наслідків аварійної ситуації. Далі проводиться розслідування причин виникнення аварійної ситуації, встановлюються винні, проводяться заходи щодо попередження виникнення подібних ситуацій надалі.

5.3 При травмуванні Працівника в наслідок ураження струмом, необхідно негайно відключити джерело струму ураження, сповістити безпосереднього начальника, викликати швидку та надати постраждалому першу медичну допомогу. Далі проводиться розслідування причин виникнення аварійної ситуації, встановлюються винні, проводяться заходи щодо попередження виникнення подібних ситуацій надалі.

5.4 При руйнуванні робочого місця в наслідок техногенних причини, Працівник має негайно покинути робоче місце, сповістити про випадок свого безпосереднього начальника. Начальник приймає рішення про подальші дії стосовно

пошкодженого робочого місці. Далі проводиться розслідування причин виникнення аварійної ситуації, встановлюються винні, проводяться заходи щодо попередження виникнення подібних ситуацій надалі.

5.5. Висновки до розділу 5

Проаналізовано шкідливі та небезпечні фактори при експлуатації «Системи контролю доступом». Проведено розрахунок та розробку інженерно-технічних заходів з охорони праці при розробці системи контролю доступу. Сформовані рекомендації щодо пожежної безпеки. Оформлена інструкція з охорони праці.

ВИСНОВКИ

В дипломній роботі була розроблена архітектура та алгоритмічне забезпечення системи доступу до приміщень з використанням штучного інтелекту.

Проведено аналіз існуючих методів контролю доступу для приміщень, їх переваги та недоліки. Проведено огляд систем контролю доступу та наявний стан ринку.

На основі проведеного аналізу можна зробити висновок, що системи контролю доступу це складні та багатокомпонентні системи. Також неможливо створити універсальну систему, що буде задовольняти потреби малого, середнього та великого бізнесу, а також потреби фізичних осіб. Тому перспективним вбачається метод, що грунтується на аналізі даних з наявних систем контролю доступу із застосуванням методів штучного інтелекту для реалізації механізму виявлення загроз та небезпечних ситуацій.

Розглянуто методи інтелектуального аналізу даних. Наведено переваги та недоліки методів машинного навчання. Обгрунтовано використання нейронних мереж для поставленної задачі, яка полягає в виявленні загроз та небезпечних ситуацій.

Для розробки алгоритмічного забезпечення було використоване сучасне програмне забезпечення, а саме PyCharm для програмування на python та бібліотеками чисельного обчислення Theano та глибинного навчання Keras і Tensorflow.

Описано роботу методу Random Forest, його переваги та недоліки. Розроблено алгоритмічне забезпечення та наведено покрокове пояснення навчання нейронної мережі. Проведена верифікація нейронної мережі, результати представлені у вигляді факторної таблиці.

Проведено аналіз впливу інформаційних технологій, зокрема центрів обробки даних, на навколишнє середовище. В результаті встановлено, що в найближчі роки швидкого зростання споживання електроенергії центрами обробки даних не передбачається. Але обсяг обчислень буде рости безперервно ще багато десятиліть, так що енергоспоживання в ЦОД необхідно контролювати. Рекомендується стежити за дотриманням стандартів, таких як Energy Star, для серверів, сховищ і мережевих

пристроїв, вимагати такої сертифікації для державних закупівель. Виробникам обладнання потрібно створити стимули для продовження випуску інноваційних енергоефективних продуктів.

Проаналізовано шкідливі та небезпечні фактори при експлуатації «Системи контролю доступом». Проведено розрахунок та розробку інженерно-технічних заходів з охорони праці при розробці системи контролю доступу. Сформовані рекомендації щодо пожежної безпеки. Оформлена інструкція з охорони праці.

СПИСОК ЛІТЕРАТУРИ

1. Eugene Schultz, E. «Risks due to convergence of physical security systems and information technology environmentsб» Information Security Technical Report, vol. 12, no. 2, pp. 80–84, 2007.
2. Garcia, Mary Lynn «Design and Evaluation of Physical Protection Systems» Butterworth-Heinemann. pp. 1–11, 2007.
3. Pereira, Henrique G. G.; Fong, Philip W. L. «SEPD: An Access Control Model for Resource Sharing in an IoT Environment,» Computer Security – ESORICS 2019. Lecture Notes in Computer Science. Springer International Publishing, no. 11736, pp. 195-216, 2019.
4. KisiBlog, [Online]. Available: https://www.getkisi.com/blog/top-10-best-access-control-software.
5. Kisi, [Online]. Available: https://www.getkisi.com.
6. ISONAS, [Online]. Available: https://www.isonas.com.
7. Johnson Controls, [Online]. Available: https://www.johnsoncontrols.com.
8. ADT, [Online]. Available: https://www.adt.com.
9. Vanderbilt Industries, [Online]. Available: https://vanderbiltindustries.com.
10. S. Laxman та S. P. Sastry, «A survey of temporal data mining,» Sadhana, vol. 31, no. 2, pp. 173-198, 2005.
11. Silberschatz, H. Korth and S. Sudarshan, Database system concepts, New York: McGraw-Hill, 2011.
12. H. Witten та F. Eibe, Data Mining: Practical Machine Learning Tools and Techniques, Morgan Kaufmann, 2011.
13. V. Hodge and J. Austin, "A survey of outlier detection methodologies," Artificial Intelligence Review, vol. 22, no. 2, pp. 85-126, 2004.
14. P. Cunningham, M. Cord та S. J. Delany, «Supervised Learning,» в Machine Learning Techniques for Multimedia: Case Studies on Organization and Retrieval, Springer Berlin Heidelberg, 2008, pp. 21-49.

15. N. Siddique та H. Adeli, «Evolutionary Neural Networks,» в Computational Intelligence: Synergies of Fuzzy Logic, Neural Networks and Evolutionary Computing, Wiley, 2013, pp. 307-355.
16. O. Chapelle, B. Schölkopf та A. Zien, Semi-Supervised Learning. Adaptive Computation and Machine Learning series., Cambridge: The MIT Press, 2006, p. 528.
17. S. S. Khan and M. G. Madden, "A survey of recent trends in one class," in Artificial Intelligence and Cognitive Science, Springer Berlin, 2010, pp. 188-197.
18. P. J. Rousseeuw and A. M. Leroy, Robust Regression and Outlier Detection, New York: Wiley-Interscience, 1987, p. 329.
19. S. Hawkins, H. He, G. Williams and R. Baxter, "Outlier detection using replicator neural networks," in 4th International Conference on Data Warehousing and Knowledge Discovery, 2002.
20. E. A., Introduction to Machine Learning, MIT Press, 2014.
21. Špica International [Online]. Available: https://www.spica.com.
22. S. Bahrampour, N. Ramakrishnan, L. Schott and M. Shah, "Comparative Study of Deep Learning Software Frameworks," 2016. [Online]. Available: https://arxiv.org/abs/1511.06435.
23. Bergstra, O. Breuleux, F. Bastien and P. Lamblin, "Theano: a CPU and GPU Math Expression Compiler," in Proceedings of the Python for Scientific Computing Conference (SciPy), Austin, TX, USA, 2010.
24. M. Abadi, A. Agarwal та P. Barham, «TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems,» в Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI ’16), Savannah, GA, USA, 2016.
25. F. Chollet, «Keras,» 2015. [Online]. Available: https://github.com/fchollet/keras.
26. D. Hunter, H. Yu, M. S. Pukish III, J. Kolbusz and B. M. Wilamowski, "Selection of proper neural network sizes and architectures: a comparative study," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 2, pp. 228-240, 2012.

27. Джигирей В.С. "Охорона навколишнього середовища" Навчальний посібник / К.: Знання, 2006.- 319 с.
28. Бойчук Л Д., Соломенно Е.М., Бугай О.В. Екологія і охорона навколишнього середовища: Навч. посіб. — Суми: Університетська книга, 2003. — 284 с.
29. Сухарев С М., Чудак С О., Сухарева О.Ю. Технологія та охорона навколишнього середовища: Навч. посіб. — Львів: Новий Світ — 2000, 2004. — 256 с.
30. Eric Masanet, Arman Shehabi, Nuoa Lei, Sarah Smith and Jonathan Koomey, “Recalibrating global data center energy-use estimates,” Science, vol 367, 2020, pp. 984-986
31. ГОСТ-12.0.003-74. Небезпечні та шкідливі виробничі фактори. 1974 г.
32. СНиП-23-05-95. Природне та штучне освітлення. 1995 г.
33. ДСанПіН-3.3.2-007-98. Гігієнічні вимоги до організації роботи з візуальними дісплейними терміналами електронно-обчислювальних машин. 1998 г.
34. СП-12.13130.2009. Визначення категорій приміщень, будинків та зовнішніх установок за вибохопожежною та пожежною небезпекою. 2009 г.