ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Удосконалення засобів захисту корпоративних комп'ютерних мереж за допомогою технології computer vision»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Кирило Будкін Павлович*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач(ка) вищої освіти гр. КІД-42
Кирило Будкін
Ім'я, ПРІЗВИЩЕ
Керівник: Андрій Лемешко
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
_____Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Будкін Кирило Павлович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: _____
керівник кваліфікаційної роботи Лемешко Андрій,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «__ _____» _____2024р. № _____
2. Строк подання кваліфікаційної роботи «_____» _____ 2024р.
3. Вихідні дані до кваліфікаційної роботи: _____
_____
_____
_____
_____
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. _____
2. _____
3. _____
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «_____» _____ 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	26.02-22.03.2024	Виконано
2	Обробка матеріалу	23.03-05.04.2024	Виконано
3	Розробка теоретичної частини	06.04-10.04.2024	Виконано
4	Розробка корпоративної мережі	11.04-30.04.2024	Виконано
5	Написання коду	01.05-03.05.2024	Виконано
6	Висновки	04.05-08.05.2024	Виконано
7	Розробка презентації	09.05-11.05.2024	Виконано
8	Передзахист	14.05-17.05.2024	Виконано
9	Здача в деканат	25.05-3.06.2024	Виконано

Здобувач(ка) вищої освіти _____ Будкін Кирило
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Лемешко Андрій
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 50 стор., 2 рис., 11 джерел.

Мета роботи – дослідження та розробка інноваційних методів для підвищення безпеки корпоративних комп’ютерних мереж шляхом використання технологій computer vision.

Об’єкт дослідження – інфраструктура корпоративної комп’ютерної мережі з computer vision.

Предмет дослідження – застосування технологій computer vision в контексті кібербезпеки.

Короткий зміст роботи: Робота починається з вступу, в якому обґрунтовується актуальність обраної теми та формулюються цілі та завдання дослідження. Потім проводиться огляд основних понять та методів комп'ютерного зору, включаючи його застосування у різних галузях, у тому числі у безпеці та відеоспостереженні. Розглядаються можливості використання технології для виявлення та запобігання кібератакам. Проектується архітектура системи, розробляються алгоритми обробки зображень та аналізу даних, а також створюється програмне забезпечення для взаємодії з обладнанням комп'ютерного зору.

КЛЮЧОВІ СЛОВА: КОМП’ЮТЕРНИЙ ЗІР, COMPUTER VISION, OPENCV, КОРПОРАТИВНА МЕРЕЖА.

ЗМІСТ

ВСТУП

Актуальність досліджуваної проблеми полягає в тому, що з розвитком конкуренції значного поширення набули такі злочини, як викрадання інформації через комп’ютерні мережі і прослуховування ліній зв’язку. З ростом кіберзагроз, які стають все більш складними та вдосконаленими завдяки розвитку технологій, важливо постійно удосконалювати методи захисту. Використання технології computer vision в цьому контексті може допомогти виявляти нові методи атак та забезпечувати більш ефективну захист корпоративних мереж. Технологія computer vision завдяки розвитку алгоритмів машинного навчання та обробки зображень стала значно потужнішою та доступнішою, що відкриває нові можливості для створення систем виявлення та запобігання кібератак. Для ефективного протидії сучасним кіберзагрозам, які відбуваються в реальному часі, важливо мати системи, що можуть реагувати миттєво на аномальні події. Технологія computere vision може стати ефективним інструментом для виявлення таких подій в реальному часі. Захист корпоративних даних, які містять значну кількість конфіденційної інформації, є критично важливим для бізнесу. Інноваційні методи захисту, такі як технологія computere vision, можуть допомогти забезпечити безпеку цих даних. У цілому, використання технології computere vision для вдосконалення захисту корпоративних комп'ютерних мереж має великий потенціал у сучасному цифровому середовищі**.** В сучасному інформаційному суспільстві, де комп'ютерні мережі стають невід'ємною складовою бізнес-процесів практично в усіх сферах діяльності, захист цих мереж стає проблемою критичного значення. В умовах постійних кіберзагроз та широкого спектру атак, важливо постійно вдосконалювати методи і засоби захисту, щоб забезпечити надійність, конфіденційність та цілісність корпоративних інформаційних ресурсів. Одним з потенційних напрямків удосконалення засобів захисту корпоративних комп'ютерних мереж є використання технології computere vision, яка здатна розпізнавати, аналізувати та виявляти аномальну поведінку та потенційні загрози в реальному часі. Використання computere vision може значно посилити можливості виявлення і

реагування на загрози, надаючи системам безпеки більш високу точність та швидкість реакції. Метою даного дипломного проекту є дослідження можливостей використання технології computere vision для удосконалення засобів захисту корпоративних комп'ютерних мереж. Проект передбачає аналіз сучасних методів захисту, вивчення основ computere vision та розробку інноваційних підходів до виявлення потенційних загроз та аномальної активності у мережах підприємств. У результаті проведених досліджень та розробок очікується створення ефективної системи захисту, яка забезпечить підвищену безпеку корпоративних мереж і внесе свій вагомий внесок у розвиток сучасних методів і засобів інформаційної безпеки.

РОЗДІЛ 1. УДОСКОНАЛЕННЯ ЗАХИСТУ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ COMUTER VISION: АНАЛІЗ, ПІДХОДИ ТА ОБҐРУНТУВАННЯ ВИБОРУ

1.1 Основні поняття та технології комп'ютерних мереж

Комп'ютерні мережі є важливою складовою інформаційного суспільства, забезпечуючи зв'язок і обмін даними між комп'ютерами та іншими пристроями. Розуміння основних понять і технологій комп'ютерних мереж є ключовим для ефективного проектування, розгортання та управління цими системами. Велике розмаїття технологій та стандартів дозволяє створювати мережі різного розміру і масштабу, від невеликих домашніх мереж до великих корпоративних інфраструктур. Однією з основних складових комп'ютерних мереж є їх архітектура. Архітектура мережі визначає організацію компонентів мережі та їх взаємозв'язки. Це включає в себе типи з'єднань (провідні, безпровідні), типи пристроїв (комп'ютери, маршрутизатори, комутатори), а також топологію мережі (зірка, шина, кільце). Розуміння архітектури допомагає забезпечити ефективне функціонування мережі та підвищити її надійність. Ще одним важливим аспектом є протоколи мережі, які визначають правила обміну даними між пристроями у мережі. Протоколи можуть бути відповідальними за різні функції, такі як передача даних, маршрутизація, забезпечення безпеки тощо. Наприклад, протоколи Ethernet і Wi-Fi використовуються для передачі даних у провідних і безпровідних мережах відповідно. Розуміння різних протоколів дозволяє вибрати найбільш підходящі для конкретної мережі. Забезпечення безпеки є ще однією ключовою складовою комп'ютерних мереж. З урахуванням постійного зростання загроз кібербезпеки, захист інформації у мережі стає дедалі важливішим завданням. Це включає в себе застосування шифрування, брандмауерів, систем виявлення вторгнень та інших заходів безпеки. Розуміння принципів і технологій безпеки допомагає забезпечити конфіденційність, цілісність та доступність даних у мережі.

Таким чином, основні поняття і технології комп'ютерних мереж включають в себе архітектуру мережі, протоколи комунікації та заходи безпеки. Розуміння цих аспектів допомагає забезпечити ефективне функціонування та захист мережі в сучасному інформаційному середовищі. Для ефективного проектування, розгортання та управління комп'ютерними мережами також важливо розглянути питання скалярність мережі, її пропускну здатність та адміністрування. Скалярність визначає здатність мережі розширюватися та пристосовуватися до зростання обсягів даних та користувачів. Пропускна здатність визначає максимальну швидкість передачі даних у мережі і важлива для забезпечення високої продуктивності. Адміністрування включає в себе управління мережевими ресурсами, налаштування пристроїв, моніторинг діяльності та вирішення проблем. Правильне розуміння цих аспектів допоможе забезпечити оптимальну продуктивність, надійність та безпеку комп'ютерних мереж у сучасному інформаційному середовищі. Тако ж Скалярність мережі є важливим аспектом, оскільки вона визначає, наскільки ефективно мережа може розширюватися та пристосовуватися до зростання обсягів даних та користувачів. Чим краще забезпечена скалярність мережі, тим більш гнучкою та відповідальною вона є до змін у вимогах та обсягах трафіку. Наприклад, якщо компанія збільшує кількість працівників або виробничих процесів, це може призвести до збільшення обсягів даних, які потрібно пересилати через мережу. Якщо мережа має гарну скалярність, вона зможе швидко адаптуватися до змін та забезпечити додаткові ресурси для задоволення нових вимог. Недостатня скалярність може призвести до перевантаження мережі, що спричинить збої у роботі, втрату даних та зниження продуктивності. Таким чином, ефективність комп'ютерних мереж безпосередньо залежить від їх скалярності, яка дозволяє адаптуватися до змін, забезпечувати стабільну роботу та оптимальну швидкість передачі даних навіть при зростанні обсягів трафіку.

1.2 Аналіз існуючих методів захисту корпоративних комп'ютерних мереж

Досліджено впровадження систем управління інформаційною безпекою в організації. Комп’ютерні мережі були визнані важливими інформаційними активами. Забезпечення цілісності їх властивостей досягнуто підбором відповідних заходів і засобів. Для цього оцінюється ризик безпеки комп’ютерної мережі та приймається рішення про необхідність обробки. Проаналізовано останні дослідження та публікації, зосереджені на узагальненій оцінці ризиків інформаційної та кібербезпеки. Часто не враховують особливості збереження властивостей активів, наприклад комп’ютерних мереж. Тому розглянуто типовий приклад подання їх структури, визначено характерні зони та елементи безпеки всередині кожної. Наслідки реалізації загроз, таких як властивості конфіденційності, цілісності та доступності, були продемонстровані на прикладах. Це дозволило ідентифікувати потенційні зони прояву ризиків безпеки комп’ютерної мережі за рівнями моделі взаємодії відкритих систем. Проаналізовано методи оцінки величини ризику та встановлено особливості використання кожного з них. Це передбачає визначення рівнів зв’язку та експлуатації, доступу, контролю над активами та врахування поєднання суб’єктивних і об’єктивних факторів в умовах невизначеності. Крім того, розглядається кореляція вузлів з їх робочим середовищем. Можливі напрямки реалізації загроз через мережеві вразливості відображаються на графіку атак. Проблема необхідності додаткової інформації про них вирішується шляхом розгляду нечіткості та невизначеності. Крім того, було виділено аспекти оцінки ризику безпеки комп’ютера. Однак, аналізуючи існуючі методи оцінки ризиків, було виявлено, що вони здебільшого зосереджені на виконанні часткових завдань, зокрема на ідентифікації та оцінці ризиків. Необхідно звернути увагу на порівняння результатів оцінки з прийнятним рівнем, обмеживши прийняття рішень та обґрунтування необхідності управління ризиками. Крім того, розглянуто властивості інформації та моделі рівнів взаємодії відкритих систем при її передачі та захисті в комп’ютерній мережі. У сучасну епоху цифрових технологій корпоративні комп’ютерні мережі знаходяться під постійною загрозою з різних

джерел, включаючи хакерів, зловмисне програмне забезпечення та внутрішні загрози. З розвитком технологій зростають і методи, які використовують зловмисники для зламу цих мереж, тому організаціям необхідно впровадити надійні заходи безпеки для захисту своїх даних, інфраструктури та репутації. У цьому аналізі ми вивчимо існуючі методи, які використовують організації для захисту своїх корпоративних комп'ютерних мереж, підкресливши їхні сильні та слабкі сторони та тенденції розвитку. Брандмауери: брандмауери діють як бар'єр між внутрішньою мережею компанії та зовнішніми загрозами. Вони перевіряють вхідний і вихідний мережевий трафік і визначають, дозволити чи заблокувати його на основі попередньо визначених правил безпеки. Хоча традиційні брандмауери ефективні для блокування відомих загроз, вони можуть протистояти новішим, складнішим атакам. Брандмауери наступного покоління (NGFW) включають додаткові функції, такі як запобігання вторгненням, розпізнавання програм і розширене виявлення загроз, щоб забезпечити кращу безпеку. Системи виявлення та запобігання вторгненням (IDPS): IDPS призначені для виявлення та запобігання зловмисній активності в мережі. Вони аналізують мережевий трафік і системні журнали в реальному часі, шукаючи ознаки підозрілої поведінки або відомі шаблони атак. IDPS може допомогти організаціям швидко виявити інциденти безпеки та реагувати на них, мінімізуючи вплив порушень. Однак вони можуть генерувати хибні спрацьовування або негативи, вимагаючи постійного налаштування та обслуговування, щоб залишатися ефективними. Безпека кінцевих точок: рішення безпеки кінцевих точок захищають окремі пристрої, такі як ноутбуки, настільні комп'ютери та мобільні пристрої, від зловмисного програмного забезпечення, несанкціонованого доступу та інших загроз. Ці рішення часто включають антивірусне програмне забезпечення, брандмауери на основі хоста та шифрування пристрою. З розвитком політики віддаленої роботи та використання власного пристрою (BYOD) безпека кінцевих точок стає все більш важливою для захисту корпоративних мереж. Однак керування та забезпечення безпеки різноманітних кінцевих точок може бути складним для IT-команд. Шифрування. Шифрування має важливе значення для захисту даних як під час

передачі, так і в стані спокою. Перетворюючи конфіденційну інформацію на зашифрований текст, який можна розшифрувати лише за допомогою правильного ключа дешифрування, шифрування допомагає запобігти несанкціонованому доступу, навіть якщо дані перехоплено. Впровадження надійних протоколів шифрування та методів керування ключами має вирішальне значення для підтримки безпеки корпоративних мереж. Однак шифрування не захищає від усіх типів атак, таких як соціальна інженерія чи внутрішні загрози. Віртуальні приватні мережі (VPN): VPN створюють безпечне зашифроване з'єднання між пристроєм користувача та корпоративною мережею, що дозволяє віддаленим співробітникам безпечно отримувати доступ до ресурсів компанії через Інтернет. VPN особливо цінні для збереження приватності та конфіденційності під час доступу до конфіденційної інформації з ненадійних мереж, таких як загальнодоступні точки доступу Wi-Fi. Проте VPN можуть додатково ускладнити мережеву інфраструктуру та бути вразливими до певних типів атак, наприклад атак типу "людина посередині". Управління інформацією про безпеку та подіями (SIEM): системи SIEM збирають і аналізують дані журналу з різних джерел у мережі організації, що дозволяє групам безпеки виявляти інциденти безпеки та реагувати на них ефективніше. Корелюючи події та виявляючи аномалії, рішення SIEM допомагають організаціям виявляти та пом'якшувати загрози в реальному часі. Однак реалізації SIEM вимагають ретельної конфігурації та постійного обслуговування, щоб гарантувати, що вони надають точну та дієву інформацію. Автентифікація користувачів і контроль доступу. Такі механізми автентифікації користувачів, як паролі, біометрія та багатофакторна автентифікація (MFA), відіграють важливу роль у контролі доступу до корпоративних мереж і ресурсів. Суворі методи автентифікації допомагають запобігти проникненню неавторизованих користувачів і обмежити потенційний вплив скомпрометованих облікових даних. Однак автентифікація користувачів настільки ж безпечна, наскільки безпечна її реалізація, і організації повинні навчати користувачів найкращим практикам, щоб уникнути поширених пасток, таких як повторне використання або обмін паролями. Навчання з питань безпеки: людська помилка

залишається однією з найбільших вразливостей у корпоративних мережах, оскільки зловмисники часто використовують нічого не підозрюючих співробітників за допомогою таких тактик, як фішинг або соціальна інженерія. Програми навчання з питань безпеки навчають співробітників ризикам кібербезпеки та найкращим практикам, надаючи їм змогу розпізнавати потенційні загрози та ефективно реагувати на них. Однак ефективність цих програм залежить від регулярних оновлень і посилення, щоб не відставати від загроз, що розвиваються. Zero Trust Security: Zero Trust — це модель безпеки, заснована на принципі «ніколи не довіряй, завжди перевіряй». За цією моделлю доступ до ресурсів обмежений і постійно оцінюється на основі таких факторів, як ідентифікація користувача, справність пристрою та мережевий контекст, незалежно від того, чи надходить запит на доступ із внутрішньої чи зовнішньої корпоративної мережі. Архітектури нульової довіри допомагають зменшити ризик внутрішніх загроз і бокового переміщення, припускаючи, що весь мережевий трафік є ненадійним, доки не буде доведено протилежне. Хмарна безпека: оскільки все більше організацій переносять свої дані та програми в хмару, забезпечення безпеки хмарних активів стає першорядним. Хмарні рішення безпеки охоплюють ряд технологій і практик, призначених для захисту даних, програм та інфраструктури в хмарних середовищах. Вони можуть включати шифрування, ідентифікацію та керування доступом (IAM), групи безпеки мережі та хмарні платформи захисту робочого навантаження (CWPP). Однак підтримувати видимість і контролювати хмарні ресурси може бути складно, особливо в багатохмарних або гібридних хмарних середовищах. Розширене виявлення загроз: Традиційні заходи безпеки, такі як брандмауери та антивірусне програмне забезпечення, є важливими, але можуть бути недостатніми для боротьби з розвиненими загрозами, що розвиваються. Розширені рішення для виявлення загроз використовують машинне навчання, штучний інтелект (AI) і аналітику поведінки для виявлення підозрілих шаблонів і аномалій, що вказують на потенційні порушення безпеки. Аналізуючи величезні обсяги даних у режимі реального часу, ці рішення можуть ефективніше виявляти загрози та реагувати на

них, скорочуючи час перебування зловмисників у корпоративних мережах. Технологія обману: технологія обману передбачає розгортання систем-приманок, файлів і облікових даних у мережі, щоб ввести в оману та відвернути зловмисників від справжніх активів. Ці приманки, відомі як honeypots або honeytokens, призначені для залучення та заманювання зловмисників, надаючи командам безпеки цінну інформацію про їх тактику, методи та процедури (TTP). Технологія обману не тільки допомагає організаціям виявляти та перешкоджати атакам, але й служить стримуючим фактором, збільшуючи складність і ризик для потенційних зловмисників. Розвідка про загрози: розвідка про загрози відноситься до знань і розуміння, отриманих в результаті аналізу кіберзагроз і вразливостей з різних джерел, включаючи розвідку з відкритим кодом, темні веб-форуми та приватні канали загроз. Використовуючи платформи та служби аналізу загроз, організації можуть проактивно виявляти нові загрози, оцінювати їх актуальність і вплив і вживати відповідних заходів для пом'якшення. Розвідка про загрози також дає змогу організаціям підвищити рівень безпеки, розуміючи тактику, прийоми та процедури (TTP), які застосовують суб'єкти загрози. Організація безпеки, автоматизація та реагування (SOAR): платформи SOAR інтегрують технології безпеки, процеси та робочі процеси для оптимізації реагування на інциденти та діяльності з управління загрозами. Автоматизуючи повторювані завдання, організовуючи складні робочі процеси та сприяючи співпраці між командами безпеки, рішення SOAR допомагають організаціям реагувати на інциденти безпеки ефективніше та результативніше. Крім того, платформи SOAR дозволяють організаціям адаптувати та масштабувати свої операції з безпеки, щоб відповідати мінливим загрозам і викликам. Безпека контейнерів: із широким впровадженням контейнеризації та архітектури мікросервісів захист контейнерних середовищ стає все більш важливим для організацій. Рішення безпеки контейнерів допомагають зменшити ризики, пов'язані з уразливістю, неправильною конфігурацією та загрозами під час виконання в контейнерних програмах. Ці рішення надають такі можливості, як сканування вразливостей, захист під час виконання та забезпечення відповідності, щоб гарантувати безпеку та цілісність контейнерних робочих

навантажень протягом усього життєвого циклу. Безпека ланцюга постачань. Оскільки організації покладаються на сторонніх постачальників і постачальників різних продуктів і послуг, захист ланцюга поставок став критичною проблемою кібербезпеки. Атаки на ланцюг постачання, такі як компрометація ланцюга постачання та атаки на ланцюг постачання програмного забезпечення, створюють значні ризики для безпеки та стійкості організацій. Щоб пом'якшити ці ризики, організації повинні впроваджувати заходи безпеки ланцюга постачання, включаючи управління ризиками постачальника, прозорість програмного забезпечення (SBOM) і перевірку стійкості ланцюга постачання. Планування реагування на інциденти та готовність: незважаючи на всі зусилля щодо запобігання інцидентам безпеки, організації повинні бути готові ефективно реагувати на порушення. Розробка та впровадження плану реагування на інциденти має важливе значення для мінімізації впливу інцидентів безпеки та швидкого відновлення нормальної роботи. Планування реагування на інциденти передбачає визначення ролей і обов'язків, встановлення протоколів зв'язку та проведення регулярних настільних навчань і симуляцій для перевірки ефективності плану. Безперервний моніторинг і аудит: підтримка видимості та нагляду за корпоративними мережами має вирішальне значення для виявлення та реагування на загрози безпеці в режимі реального часу. Рішення для безперервного моніторингу збирають і аналізують телеметричні дані з різних джерел, включаючи мережевий трафік, кінцеві точки та хмарні середовища, для виявлення аномальної поведінки та потенційних інцидентів безпеки. Проводячи регулярні аудити та оцінки безпеки, організація NS можуть виявити прогалини та вразливі місця у своїй безпеці та вжити проактивних заходів для їх усунення. Відповідність нормативним вимогам і управління: нормативні рамки, такі як GDPR, HIPAA та PCI DSS, накладають юридичні та нормативні зобов'язання на організації щодо захисту конфіденційних даних і забезпечення безпеки та конфіденційності їхніх систем і мереж. Відповідність цим нормам не тільки допомагає організаціям уникнути юридичних санкцій і штрафів, але й сприяє довірі клієнтів і зацікавлених сторін. Впровадження надійних процесів управління та засобів контролю має важливе

значення для досягнення та підтримки нормативної відповідності в сучасному складному та динамічному середовищі загроз. Культура кібербезпеки та обізнаність: Створення сильної культури кібербезпеки в організації має фундаментальне значення для її загальної безпеки. Розвиваючи культуру поінформованості про безпеку та підзвітності, організації можуть надати співробітникам можливість розпізнавати потенційні загрози та повідомляти про них, дотримуватися політик і процедур безпеки та відігравати активну роль у захисті корпоративних мереж. Програми навчання та підвищення обізнаності з кібербезпеки мають бути адаптовані до ролей і обов'язків співробітників і регулярно підвищуватися, щоб залишатися актуальними та ефективними.

1.3 Огляд сучасних підходів до використання computer vision у сфері інформаційної безпеки

Комп'ютерний зір відіграє вирішальну роль у системах спостереження та моніторингу, дозволяючи організаціям виявляти та запобігати порушенням безпеки в реальному часі. Розширені алгоритми відеоаналітики можуть аналізувати живе відео, щоб виявити підозрілі дії, спроби несанкціонованого доступу або потенційні загрози. Технологія розпізнавання облич, зокрема, розширює можливості систем спостереження, дозволяючи ідентифікувати та відстежувати людей у різних місцях. Проте занепокоєння щодо конфіденційності та етичних наслідків спровокували дебати щодо відповідального використання розпізнавання обличчя в інформаційній безпеці. Включення комп'ютерного бачення в механізми виявлення загроз і запобігання вторгненням покращує здатність ідентифікувати та зменшувати ризики безпеки. Алгоритми виявлення аномалій використовують методи машинного та глибокого навчання для виявлення незвичайних моделей або поведінки в цифрових середовищах. Аналізуючи мережевий трафік, поведінку користувачів і системні журнали, ці алгоритми можуть виявляти потенційні порушення безпеки або зловмисні дії в реальному часі. Крім того, системи візуального огляду, оснащені можливостями комп'ютерного зору, можуть виявляти фізичні вторгнення, такі як несанкціонований доступ до зон обмеженого

доступу або втручання в камери спостереження. Традиційні методи автентифікації та контролю доступу доповнюються технологіями комп’ютерного зору для посилення заходів безпеки. Біометричні системи автентифікації, такі як розпізнавання райдужної оболонки ока та сканування вен долоні, використовують алгоритми комп’ютерного зору для перевірки особи користувачів на основі унікальних фізіологічних характеристик. Ці системи пропонують більш безпечну та зручну альтернативу традиційним паролям або PIN-кодам, зменшуючи ризик несанкціонованого доступу та крадіжки особистих даних. Проте забезпечення точності та надійності біометричних систем автентифікації залишається проблемою, особливо в різноманітних умовах навколишнього середовища та з різними демографічними характеристиками користувачів. Оскільки організації збирають і обробляють величезні обсяги візуальних даних з метою безпеки, захист конфіденційності та цілісності цих даних стає першорядним. Методи шифрування та безпечні протоколи використовуються для захисту конфіденційної інформації під час передачі та зберігання. Крім того, методи анонімізації та деідентифікації використовуються для видалення ідентифікаційної інформації із записів відеоспостереження або наборів даних зображень, зменшуючи ризик порушення конфіденційності. Однак поширення технології deepfake створює нові проблеми для автентичності та цілісності даних, підкреслюючи потребу в надійних механізмах автентифікації та інструментах цифрової криміналістики.

Інтеграція комп’ютерного бачення з пристроями Інтернету речей (IoT) і периферійними обчислювальними платформами підвищує масштабованість і швидкість реакції систем інформаційної безпеки. Обробка на основі периферії дає змогу аналізувати візуальні дані в реальному часі на периферії мережі, зменшуючи затримку та вимоги до пропускної здатності. Використовуючи алгоритми комп’ютерного зору на периферійних пристроях, таких як камери безпеки або інтелектуальні датчики, організації можуть виявляти загрози безпеці ближче до джерела та ініціювати швидке реагування. Проте забезпечення безпеки та стійкості периферійних обчислювальних інфраструктур проти кібератак залишається критичною проблемою. Широке застосування технологій комп’ютерного бачення

в інформаційній безпеці викликає етичні проблеми щодо конфіденційності, упередженості та неправильного використання. Системи розпізнавання облич, зокрема, потрапили під пильну увагу через їх потенційну можливість порушувати права особи на конфіденційність і підтримувати суспільні упередження. Такі питання, як справедливість алгоритмів, прозорість і підзвітність, мають першочергове значення для забезпечення того, щоб додатки комп'ютерного зору в сфері безпеки дотримувалися етичних принципів і поважали права людини. Крім того, занепокоєння з приводу капіталізму стеження та комерціалізації особистих даних підкреслюють необхідність нормативно-правової бази та етичних принципів для управління відповідальною розробкою та розгортанням систем комп'ютерного зору. Використання технологій комп'ютерного зору у сфері інформаційної безпеки являє собою зміну парадигми в тому, як організації захищають свої цифрові активи та інфраструктуру. Сучасні підходи до комп'ютерного зору пропонують безпрецедентні можливості для покращення заходів безпеки, від спостереження та виявлення загроз до автентифікації та захисту даних. Однак вирішення проблем етики, конфіденційності та масштабованості є важливим для реалізації повного потенціалу цих технологій у захисті конфіденційної інформації та пом'якшенні кіберзагроз. Оскільки ландшафт інформаційної безпеки продовжує розвиватися, поточні дослідження та інновації в області комп'ютерного зору відіграватимуть життєво важливу роль у формуванні майбутнього цифрової безпеки.

1.4 Обґрунтування вибору конкретних технологій computer vision

Технологія розпізнавання облич передбачає автоматизовану ідентифікацію або верифікацію осіб за цифровими зображеннями чи відеокадрами. Він покладається на складні алгоритми для аналізу рис обличчя, таких як відстань між очима, форма носа та контури обличчя. Ця технологія набула поширення в різних секторах, включаючи правоохоронні органи, роздрібну торгівлю, а тепер і корпоративну безпеку. Одним з переконливих аргументів для розгортання технології розпізнавання облич у корпоративних мережах є її здатність покращувати автентифікацію та контроль доступу. Традиційні методи автентифікації, такі як

паролі або ключ-карти, можуть бути зламані через крадіжку, втрату або неавторизоване копіювання. Однак розпізнавання обличчя пропонує біометрично безпечну альтернативу, оскільки риси обличчя кожної людини унікальні, і їх важко відтворити. Інтегруючи розпізнавання облич у системи контролю доступу, корпорації можуть забезпечити доступ до чутливих зон лише авторизованому персоналу, тим самим підвищуючи безпеку мережі. Ще однією головною перевагою технології розпізнавання обличчя є її здатність виявляти загрози в реальному часі та реагувати на них. Корпоративне середовище вразливе до різноманітних загроз безпеці, включаючи несанкціоновані вторгнення, несанкціоновані дії та внутрішні загрози. Камери розпізнавання облич, оснащені вдосконаленими алгоритмами, можуть швидко ідентифікувати зацікавлених осіб і миттєво сповіщати співробітників служби безпеки. Цей проактивний підхід дозволяє швидко втручатися, запобігаючи потенційним порушенням безпеки до того, як вони переростуть у повноцінні інциденти. Доцільність інтеграції технології розпізнавання обличчя з існуючою інфраструктурою є вирішальним питанням для корпорацій. На щастя, сучасні системи розпізнавання облич пропонують бездоганну інтеграцію з різними апаратними та програмними платформами, мінімізуючи потребу в масштабній переробці інфраструктури. Незалежно від того, розгортаються як окремі камери чи інтегруються в існуючі мережі відеоспостереження, технологія розпізнавання облич може бути налаштована відповідно до конкретних потреб і конфігурацій корпоративного середовища. Незважаючи на свою ефективність у зміцненні безпеки мережі, технологія розпізнавання облич повинна відповідати суворим нормам конфіденційності. Корпорації повинні орієнтуватися в складному ландшафті законів і норм щодо конфіденційності, включаючи GDPR в Європі та CCPA в Каліфорнії. Вибір технологій розпізнавання облич, які надають пріоритет конфіденційності за проектом, як-от забезпечення анонімності даних, управління згодою та надійні протоколи шифрування, є обов’язковим для відповідності. Віддаючи пріоритет гарантіям конфіденційності, корпорації можуть зменшити ризик регуляторних санкцій і зберегти довіру співробітників і зацікавлених сторін. Швидкі темпи

технологічних інновацій підкреслюють важливість вибору технологій розпізнавання обличчя, які є не тільки надійними, але й адаптованими до майбутніх досягнень. Корпоративні мережі з часом розвиваються, що вимагає масштабованих рішень, здатних пристосуватися до зростання та нових загроз. Вибір постачальників систем розпізнавання облич із підтвердженою репутацією інновацій і прихильністю до постійних досліджень і розробок гарантує, що корпорації залишаються на передньому краї мережевої безпеки, використовуючи передові технології для захисту своїх активів. Вибір конкретних технологій комп'ютерного зору є важливим аспектом, коли йдеться про захист корпоративних мереж з використанням можливостей розпізнавання осіб. У цьому обговоренні ми прагнемо заглибитись в обґрунтування вибору конкретних технологій у галузі комп'ютерного зору для підвищення заходів безпеки у бізнес-середовищі. При розгляді захисту корпоративних мереж за допомогою камер з функцією розпізнавання облич необхідно враховувати кілька ключових факторів. Одним із основних виправдань використання конкретних технологій комп'ютерного зору є їхня здатність пропонувати розширені можливості розпізнавання осіб з високою точністю та ефективністю. Такі технології, як алгоритми розпізнавання осіб на основі глибокого навчання, продемонстрували чудову ефективність ідентифікації та аутентифікації людей, тим самим зміцнюючи інфраструктуру безпеки корпоративних мереж. Більше того, на вибір технологій комп'ютерного зору для розпізнавання облич також впливають такі фактори, як масштабованість, гнучкість та сумісність з існуючими мережевими системами. Вибір технологій, які легко масштабуються, дозволяє підприємствам плавно розширювати свої заходи безпеки зі зростанням мережної інфраструктури. Крім того, гнучкість цих технологій дозволяє адаптувати їх до унікальних вимог різних корпоративних середовищ, забезпечуючи індивідуальний підхід до мережевої безпеки. Ще одним важливим аспектом, що впливає на вибір конкретних технологій комп'ютерного зору, є можливості їх інтеграції з мережевими компонентами. Сумісність з різноманітними апаратними та програмними системами в корпоративних мережах необхідна для безперешкодного розгортання та ефективної роботи камер

розпізнавання облич. Технології, що пропонують надійні можливості інтеграції, сприяють плавній співпраці між різними компонентами безпеки, підвищуючи загальну ефективність механізмів захисту мережі. Крім того, міркування щодо конфіденційності та безпеки даних відіграють ключову роль у визначенні придатності технологій комп'ютерного зору для захисту корпоративної мережі за допомогою розпізнавання осіб. Вибір технологій, що відповідають суворим правилам захисту даних та включають протоколи шифрування, забезпечує конфіденційність та цілісність конфіденційної інформації, отриманої камерами розпізнавання осіб. Віддаючи пріоритет функціям безпеки та конфіденційності в процесі відбору, компанії можуть знизити потенційні ризики, пов'язані з несанкціонованим доступом або неправильним використанням даних розпізнавання осіб. Насамкінець, обґрунтування вибору конкретних технологій комп'ютерного зору для захисту корпоративних мереж з використанням можливостей розпізнавання осіб є багатогранним. На процес прийняття рішень впливають різні чинники: від передових алгоритмів розпізнавання осіб до масштабованості, сумісності, інтеграції та безпеки даних. Вибираючи технології, які процвітають у цих галузях, компанії можуть посилити заходи мережної безпеки та забезпечити захист конфіденційних даних у своєму корпоративному середовищі. Підсумовуючи, інтеграція технології розпізнавання обличчя є стратегічним імперативом для корпорацій, які прагнуть посилити безпеку своєї мережі. Забезпечуючи розширену автентифікацію та контроль доступу, полегшуючи виявлення загроз у реальному часі та реагування на них, плавно інтегруючись із наявною інфраструктурою, забезпечуючи дотримання правил конфіденційності та впроваджуючи постійні інновації, технології розпізнавання облич пропонують надійний захист від різноманітних загроз безпеці. Оскільки корпорації перебувають у дедалі складнішому середовищі загроз, розумний вибір конкретних технологій комп’ютерного зору, зокрема систем розпізнавання облич, має першочергове значення для захисту корпоративних мереж і збереження організаційної цілісності в епоху цифрових технологій.

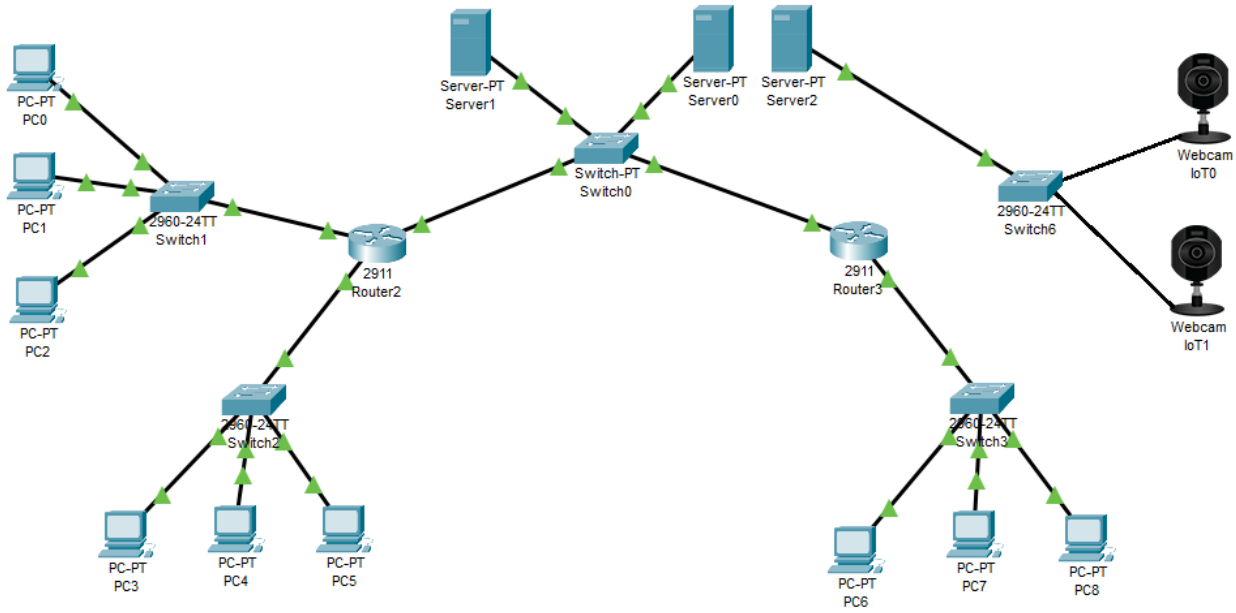
РОЗДІЛ 2. РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Архітектура системи, що розробляється

Топологія star, також відома як топологія зірка, ідеально підходить як для корпоративних, так і для домашніх мереж, оскільки має багато переваг, які дуже цінуються. У цій конфігурації всі пристрої підключені до центрального вузла, як правило, комутатора або маршрутизатора. Однією з ключових переваг топології зірок є простота управління та адміністрування. Централізована точка управління спрощує моніторинг і управління всією мережею, а також спрощує і прискорює діагностику і вирішення проблем. Несправність пристрою або кабелю впливає лише на з'єднання з центральним вузлом, тому не впливає на решту мережі. Ізоляція цієї проблеми значно підвищує загальну надійність мережі. Крім того, топологія зіроки масштабована. Додавання нового пристрою-це простий процес, який не вимагає зміни існуючої структури мережі.Новий пристрій можна просто підключити до центрального концентратора. Така гнучкість дозволяє мережі безперешкодно розвиватися відповідно до потреб організації. Продуктивність є ще однією важливою перевагою, оскільки сучасні комутатори можуть забезпечити спеціальний канал зв'язку для кожного підключеного пристрою, зменшуючи ймовірність конфліктів даних та оптимізуючи загальний мережевий трафік. Центральний вузол може ефективно управляти трафіком і забезпечувати ефективне використання мережевих ресурсів. Налаштування та налаштування початкової топології також відносно прості. Проводка проста, і кожен пристрій підключений безпосередньо до центрального вузла, тому процес стає ще простішим, якщо ви використовуєте мережеве обладнання та кабелі з більш стандартним процесом монтажу порівняно з іншими топологіями, такими як Шини та кільця. У зіркоподібній топології всі дані проходять через центральний вузол, що підвищує безпеку та покращує моніторинг та контроль мережевого трафіку. Якщо у вас є лише одна точка потоку трафіку, такі заходи безпеки, як брандмауери та системи виявлення вторгнень, простіше реалізувати. Крім того,

топологія зірок полегшує модернізацію та модернізацію вашої мережі. Удосконалення центрального вузла, такі як модернізація комутаторів і маршрутизаторів, забезпечують загальну продуктивність мережі без заміни всіх підключених пристроїв, а інтеграція нових технологій і протоколів спрощує управління за рахунок оновлення центральних компонентів. В цілому, простота управління топологією зірка, висока надійність, масштабованість, продуктивність, простота установки, підвищена безпека і простий спосіб оновлення роблять його відмінним вибором для побудови надійної та ефективної мережі. Ці переваги дозволяють мережі працювати ефективно, адаптуватися до зростання та підтримувати високі стандарти продуктивності та безпеки. Централізована структура топології зірка не тільки полегшує управління, але й забезпечує значні переваги з точки зору обслуговування мережі та усунення несправностей. Усі пристрої підключені до центрального концентратора, тому адміністратори мережі можуть легко ізолювати та усунути проблеми, не впливаючи на всю мережу. Це скорочує час простою і дозволяє мережі продовжувати працювати, навіть якщо окремі компоненти виходять з ладу. Крім того, топологія зірки підтримує кращий розподіл ресурсів та балансування навантаження. Централізовані вузли можуть розумно керувати трафіком даних, запобігаючи вузьким місцям та оптимізуючи продуктивність підключених пристроїв. Ще однією важливою перевагою топології зірки є її сумісність з широким спектром мережевих технологій.1 він може бути легко інтегрований як з дротовими, так і з бездротовими мережами, універсальний і адаптується до різних умов. Ця адаптивність особливо корисна для зростаючих організацій, яким потрібно масштабувати свою мережеву інфраструктуру без капітального ремонту. Топологія зірки також полегшує реалізацію мережевої політики та контролю доступу. Централізувавши контрольні точки, адміністратори мережі можуть застосовувати заходи безпеки, відстежувати активність користувачів та ефективніше керувати дозволами.

Що стосується витрат, початкове налаштування початкової топології може бути високим через необхідність центрального концентратора та окремого підключення для кожного пристрою, але довгострокові вигоди часто перевищують ці витрати. Поєднання скорочення часу обслуговування і простоїв, а також простота додавання нових пристроїв роблять його економічно ефективним рішенням в довгостроковій перспективі. Крім того, використання стандартного мережевого обладнання та кабелів Жовтневої топології може призвести до економії обладнання та зменшити складність управління запасами. В освітніх та бізнес-середовищах, де надійність та продуктивність мережі мають вирішальне значення, Startup topology пропонує надійне рішення. Він підтримує додатки з високою пропускною здатністю і забезпечує ефективну і надійну передачу даних. Це особливо важливо в Налаштуваннях, де кілька користувачів і пристроїв потребують одночасного доступу до ресурсів без шкоди для продуктивності. Топологія зірок також сприяє покращенню планування та масштабованості мережі.



2.2 Реалізація основних компонентів системи

Звичайно, почнемо зі списку пристроїв:

Сервера:
Маршрутизатор із інтегрованими службами Cisco серії ISR 4000
Комутатор Cisco Catalyst серії 9000

Маршрутизатори:
Маршрутизатор із інтегрованими службами Cisco серії ISR 1000
Маршрутизатор із інтегрованими службами Cisco серії ISR 4000
Маршрутизатор служб агрегації серії Cisco ASR 1000

У сфері корпоративних мереж вибір правильного обладнання є найважливішим. Ефективність, масштабованість і безпека мережевої інфраструктури безпосередньо залежать від вибору пристроїв. У межах архітектури мережі вибір сервера миші та маршрутизаторів відіграє ключову роль у визначенні загальної продуктивності та надійності. У цьому дискурсі ми дослідимо обґрунтування вибору маршрутизатора з інтегрованими послугами серії Cisco ISR 4000 і комутатора Cisco Catalyst серії 9000 як сервера миші, а також маршрутизатора з інтегрованими послугами Cisco ISR 1000, маршрутизатора з інтегрованими послугами Cisco ISR 4000 і Cisco Маршрутизатор служб агрегації серії ASR 1000 як маршрутизатор для нашої корпоративної мережі, реалізований у Cisco Packet Tracer.

Перш за все, давайте звернемося до сервера миші. Сервер миші є критично важливим компонентом інфраструктури корпоративної мережі, відповідальним за централізацію таких ресурсів, як файли, принтери та програми. Він діє як концентратор, полегшуючи спілкування та обмін даними між різними пристроями в мережі. У нашому контексті маршрутизатор Cisco серії ISR 4000 Integrated Services Router і комутатор Cisco Catalyst серії 9000 є ідеальними кандидатами на цю роль.

Маршрутизатор із інтегрованими послугами серії Cisco ISR 4000 відомий своєю надійною продуктивністю, розширеними функціями безпеки та масштабованістю. Серія ISR 4000, оснащена багатоядерними процесорами та інтегрованими сервісними модулями, забезпечує високу пропускну здатність і низьку затримку, що робить її ідеальною для роботи з високим навантаженням корпоративного сервера миші. Його модульна конструкція дозволяє легко розширюватися, враховуючи майбутнє зростання та технологічний прогрес, не вимагаючи повної реконструкції інфраструктури.

Доповнюючи серію ISR 4000, комутатор Cisco Catalyst серії 9000 надає передові можливості з точки зору керування мережею, безпеки та автоматизації. Завдяки програмованій архітектурі та підтримці програмно-визначеного доступу (SD-доступу) серія Catalyst 9000 спрощує мережеві операції та підвищує гнучкість. Крім того, його вбудовані функції безпеки, такі як шифрування MACsec і TrustSec, зміцнюють загальну безпеку мережі, захищаючи конфіденційні дані від несанкціонованого доступу та кіберзагроз.

Переходячи до маршрутизаторів, ці пристрої служать магістралью мережі, відповідальною за спрямування трафіку між різними сегментами, оптимізацію продуктивності та забезпечення з’єднання. Вибір маршрутизаторів має вирішальне значення, оскільки вони визначають ефективність і надійність передачі даних у мережі. Для нашої корпоративної мережі поєднання маршрутизатора з інтегрованими службами Cisco ISR 1000 Series, Cisco ISR 4000 Series Integrated Services Router і Cisco ASR 1000 Series Aggregation Services Router пропонує комплексне рішення, адаптоване до наших вимог.

Починаючи з Cisco ISR 1000 Series Integrated Services Router, цей компактний, але потужний маршрутизатор призначений для малих і середніх підприємств, пропонуючи ідеальний баланс між продуктивністю та доступністю. Інтегровані

функції безпеки, включаючи шифрування VPN і захист від загроз, забезпечують безпечний шлюз для віддаленого підключення та розгортання філій. Завдяки підтримці програмно визначеної WAN (SD-WAN) і маршрутизації з урахуванням додатків серія ISR 1000 оптимізує продуктивність додатків і використання пропускної здатності, забезпечуючи безперебійну роботу користувача в мережі.

Наріжним каменем ядра нашої мережевої інфраструктури є маршрутизатор із інтегрованими послугами серії Cisco ISR 4000. Відома своєю масштабованістю та універсальністю, серія ISR 4000 задовольняє різноманітні потреби мереж корпоративного рівня, легко обробляючи великі обсяги трафіку. Його інтегрована архітектура послуг об'єднує численні функції в єдину платформу, спрощуючи керування та знижуючи експлуатаційні витрати. Крім того, завдяки підтримці розширених протоколів маршрутизації, таких як OSPF, BGP і EIGRP, серія ISR 4000 забезпечує неперевершену гнучкість і стійкість, забезпечуючи динамічну адаптацію до мінливих умов мережі.

І останнє, але не менш важливе: маршрутизатор Cisco ASR 1000 Series Aggregation Services Router зміцнює мережеву інфраструктуру своєю неперевершеною продуктивністю та надійністю. Серія ASR 1000, розроблена для великомасштабного розгортання та середовищ центрів обробки даних, чудово справляється з додатками та послугами, які потребують великої пропускної здатності. Його архітектура операторського класу, що базується на багатоядерних процесорах і високошвидкісних інтерфейсах, забезпечує плавну та безперебійну роботу навіть за великих навантажень. Крім того, завдяки таким функціям, як якість обслуговування (QoS) і формування трафіку, серія ASR 1000 визначає пріоритет критичного трафіку та підтримує оптимальну продуктивність у мережі, покращуючи загальний досвід роботи з користувачем.

На завершення вибір маршрутизатора з інтегрованими службами Cisco ISR 4000 і комутатора Cisco Catalyst 9000 як сервера миші, а також маршрутизатора з

інтегрованими послугами Cisco ISR 1000, маршрутизатора з інтегрованими послугами Cisco ISR 4000 та агрегації Cisco ASR 1000 Services Router, як і маршрутизатори, керується поєднанням продуктивності, масштабованості та міркувань безпеки. Ці пристрої не тільки задовольняють поточні потреби нашої корпоративної мережі, але й забезпечують міцну основу для майбутнього розширення та технологічного прогресу. Завдяки розширеним функціям і надійним можливостям вони забезпечують безперебійну роботу та цілісність нашої мережевої інфраструктури, що дозволяє нашій організації процвітати в сучасному динамічному бізнес-ландшафті.

Реалізація протоколу динамічної конфігурації хоста (DHCP) і протоколу мережевого часу (NTP) є невід'ємною частиною функціональності та ефективності сучасних корпоративних мереж. DHCP спрощує адміністрування мережі шляхом автоматизації призначення IP-адрес та інших параметрів мережевої конфігурації пристроям, тоді як NTP забезпечує точну синхронізацію часу між мережевими пристроями, сприяючи узгодженим операціям і забезпечуючи точне ведення журналів і кореляцію подій. Тут я опишу впровадження протоколів DHCP і NTP у корпоративній мережі, охоплюючи конфігурацію, розгортання та найкращі практики.

Реалізація протоколу динамічної конфігурації хоста (DHCP):

DHCP відіграє вирішальну роль в управлінні мережею, динамічно розподіляючи IP-адреси та інші параметри конфігурації мережі клієнтським пристроям.

Щоб реалізувати DHCP у корпоративній мережі:

Розгорніть один або кілька DHCP-серверів у межах мережевої інфраструктури. Ці сервери можуть бути автономними пристроями або інтегрованими в існуючі маршрутизатори чи комутатори. Налаштуйте сервер DHCP за допомогою пулу IP-адрес, масок підмережі, адрес шлюзу за замовчуванням, адрес DNS-сервера та інших відповідних параметрів. Визначте області DHCP, щоб визначити діапазон IP-адрес, доступних для призначення клієнтським пристроям у кожній підмережі.

Конфігурація агента ретрансляції DHCP (за наявності):

Якщо запити DHCP потрібно пересилати через кілька підмереж, налаштуйте агенти ретрансляції DHCP на маршрутизаторах або комутаторах рівня 3 для ретрансляції повідомлень DHCP між клієнтами та серверами DHCP. Укажіть IP-адресу DHCP-сервера(ів), на який мають пересилатися запити DHCP.

Конфігурація клієнта:

Налаштуйте клієнтські пристрої для динамічного отримання параметрів мережі через DHCP. Зазвичай це можна зробити через параметри мережі пристрою або конфігурацію клієнта DHCP.

Переконайтеся, що DHCP увімкнено на клієнтських пристроях і налаштовано на автоматичне отримання IP-адрес.

Моніторинг і технічне обслуговування:

Відстежуйте продуктивність і використання сервера DHCP, щоб забезпечити оптимальний розподіл ресурсів і вирішити будь-які потенційні проблеми.

Регулярно переглядайте інформацію про оренду DHCP і статистику розподілу адрес, щоб виявити й усунути будь-які потенційні конфлікти чи неефективність.

Застосуйте заходи безпеки DHCP, такі як відстеження DHCP і контроль доступу до DHCP-сервера, щоб запобігти несанкціонованому спуфінгу DHCP-сервера або несанкціонованому розгортанню DHCP-сервера.

Реалізація мережевого протоколу часу (NTP):

Протокол NTP забезпечує точну синхронізацію часу між мережевими пристроями, що має вирішальне значення для підтримки узгодженості журналювання, кореляції подій і мережевих операцій. Щоб реалізувати NTP в корпоративній мережі:

Конфігурація сервера NTP:

Розгорніть один або кілька NTP-серверів у межах мережевої інфраструктури. Ці сервери можуть синхронізувати час із зовнішніми серверами NTP або використовувати локальні джерела часу, такі як GPS або атомний годинник.

Налаштуйте NTP-сервер за допомогою відповідних джерел синхронізації часу та опорних годинників, щоб забезпечити точне відображення часу.

Визначте політики NTP-сервера та засоби керування доступом, щоб обмежити синхронізацію часу лише авторизованими пристроями.

Конфігурація клієнта NTP:

Налаштуйте мережеві пристрої та сервери в мережі для синхронізації часу з сервером(ами) NTP. Укажіть IP-адресу або ім’я хоста серверів NTP, з якими пристрої мають синхронізувати свої годинники. Налаштуйте параметри клієнта NTP, щоб визначити пріоритети та вибрати найбільш надійні джерела часу для синхронізації.

Моніторинг і технічне обслуговування:

Відстежуйте продуктивність NTP-сервера та стан синхронізації, щоб забезпечити точний час і виявити будь-які проблеми синхронізації. Регулярно оновлюйте конфігурації NTP-сервера та джерела синхронізації часу, щоб підтримувати точність і надійність. Застосуйте автентифікацію та шифрування NTP, щоб захистити зв’язок синхронізації часу та запобігти несанкціонованому підробленню чи маніпулюванню часом. Реалізація протоколів DHCP і NTP у корпоративній мережі має важливе значення для ефективного керування мережею, розподілу ресурсів і синхронізації часу. Дотримуючись найкращих практик і вказівок щодо конфігурації, розгортання та обслуговування DHCP і NTP, організації можуть забезпечити безперебійну роботу мережі, точне відстеження часу та підвищену безпеку. DHCP спрощує керування IP-адресами та конфігурацію мережі, тоді як NTP забезпечує узгоджену синхронізацію часу між мережевими пристроями, сприяючи загальній надійності та функціональності інфраструктури корпоративної мережі.

2.3 Рекомендації щодо впровадження системи у корпоративні мережі

Впровадження системи в корпоративних мережах — це багатогранна робота, яка вимагає ретельного планування, ретельного виконання та постійного управління. Щоб забезпечити успіх такого починання, важливо враховувати різні чинники, починаючи від дизайну мережі та конфігурації пристрою до реалізації безпеки та дотримання вимог. У цьому вичерпному посібнику я викладу рекомендації щодо впровадження системи в корпоративних мережах, охоплюючи такі ключові аспекти, як дизайн мережі, розгортання пристроїв, заходи безпеки, планування аварійного відновлення, навчання співробітників, дотримання вимог і оптимізація продуктивності.

Міцний фундамент має вирішальне значення для будь-якої корпоративної мережі. Почніть із проведення ретельної оцінки мережевих вимог організації, враховуючи поточні потреби та прогнози щодо майбутнього зростання. Визначте топологію мережі, включаючи розміщення основних компонентів, таких як сервери миші, маршрутизатори, комутатори та точки доступу. Враховуйте такі фактори, як резервування, відмовостійкість і масштабованість, щоб створити стійку та адаптовану мережеву архітектуру.

Після завершення проектування мережі перейдіть до налаштування та розгортання мережевих пристроїв. Дотримуйтеся передових методів і інструкцій із безпеки Cisco, щоб переконатися, що кожен пристрій правильно налаштовано відповідно до вимог організації. Застосуйте надійні заходи безпеки, такі як списки контролю доступу (ACL), брандмауери та системи виявлення/запобігання вторгненням (IDS/IPS), щоб захистити від несанкціонованого доступу та кіберзагроз. Використовуйте сегментацію VLAN, щоб ізолювати трафік і підвищити безпеку, а також запровадити політики якості обслуговування (QoS), щоб визначити пріоритет критичного трафіку та оптимізувати використання пропускної здатності.

Централізоване управління та моніторинг необхідні для підтримки працездатності та продуктивності корпоративної мережі. Розгорніть платформи керування мережею, такі як Cisco DNA Center, для централізованого налаштування, моніторингу та усунення несправностей мережевих пристроїв. Використовуйте інструменти автоматизації та оркестровки, щоб оптимізувати операції та мінімізувати помилки вручну. Впроваджуйте системи проактивного моніторингу для виявлення та реагування на аномалії мережі та загрози безпеці в режимі реального часу, забезпечуючи своєчасне втручання та вирішення проблем.

Безпека має першочергове значення в корпоративних мережах, враховуючи конфіденційність даних і поширеність кіберзагроз. Застосуйте надійні механізми автентифікації, такі як багатофакторна автентифікація (MFA), щоб контролювати доступ до мережевих ресурсів і запобігати несанкціонованому доступу. Оновлюйте мережеві пристрої за допомогою оновлень програмного забезпечення та виправлень безпеки, щоб усунути відомі вразливості та зменшити ризики. Застосуйте протоколи шифрування, такі як SSL/TLS і IPsec, щоб захистити дані під час передавання та зберігання. Проводьте регулярні перевірки безпеки та тести на проникнення, щоб виявити й усунути потенційні слабкі місця в мережевій інфраструктурі.

Планування аварійного відновлення має важливе значення для забезпечення здатності організації відновлюватися після системних збоїв або кібератак і підтримувати безперервність бізнесу. Встановіть надійні механізми резервного копіювання та аварійного відновлення для захисту критично важливих даних і програм. Впроваджуйте резервні зв’язки та механізми відновлення після збоїв, щоб мінімізувати час простою та підтримувати доступність послуг у разі збоїв у мережі. Розробіть комплексні плани реагування на інциденти, щоб сприяти швидкому й ефективному реагуванню на інциденти безпеки, забезпечуючи мінімальні збої в бізнес-операціях.

Співробітники часто є найслабшою ланкою в ланцюжку безпеки, тому навчання та підвищення обізнаності співробітників є ключовими компонентами будь-якої стратегії кібербезпеки. Проводьте регулярні тренінги та програми підвищення обізнаності, щоб навчити співробітників найкращим практикам безпеки, включаючи звички безпечного перегляду, гігієни паролів і соціальної інженерії. Розвивайте культуру свідомості безпеки в організації та заохочуйте співробітників негайно повідомляти про будь-які підозрілі дії, забезпечуючи своєчасне виявлення та пом’якшення загроз безпеці.

Відповідність відповідним галузевим стандартам і нормативним вимогам не підлягає обговоренню для організацій, які працюють у строго регульованих секторах. Забезпечте відповідність таким стандартам, як GDPR, HIPAA, PCI DSS тощо, запровадивши відповідні засоби контролю безпеки та протоколи. Ведіть точну документацію та перевірку, щоб продемонструвати дотримання правових і нормативних зобов’язань. Взаємодіяйте з юридичними командами та відділами відповідності, щоб залишатися в курсі змін нормативного ландшафту та відповідним чином адаптувати політики та процедури.

Оптимізація продуктивності мережі – це постійний процес, який потребує регулярного моніторингу та тонкого налаштування. Відстежуйте показники продуктивності мережі та аналізуйте моделі трафіку, щоб виявити вузькі місця та оптимізувати використання ресурсів. Тонке налаштування мережевих конфігурацій і політик на основі контрольних показників продуктивності та бізнес-вимог. Будьте в курсі нових технологій і галузевих тенденцій, щоб визначати можливості для інновацій і вдосконалень, забезпечуючи, щоб корпоративна мережа залишалася гнучкою, ефективною та стійкою перед лицем викликів і вимог, що постійно розвиваються. Впровадження системи в корпоративних мережах є складним заходом, який вимагає ретельного планування, ретельного виконання та постійного управління. Дотримуючись

рекомендацій, викладених у цьому посібнику, організації можуть створити надійну та безпечну мережеву інфраструктуру, яка відповідає їхнім поточним потребам і може масштабуватися відповідно до майбутнього зростання та технологічного прогресу. Завдяки добре спроектованій і правильно реалізованій мережі організації можуть оптимізувати продуктивність, підвищити безпеку та підтримувати конкурентну перевагу в сучасному динамічному бізнес-середовищі.

РОЗДІЛ 3. РОЗРОБКА ТЕХНОЛОГІЇ COMPUTER VISION

3.1 Опис нейроної моделі

Створення нейронної моделі для розпізнавання обличчя за допомогою OpenCV передбачає комплексне розуміння різних методів обробки зображень, комп'ютерного зору та машинного навчання. OpenCV, бібліотека комп'ютерного зору з відкритим вихідним кодом, широко використовується для програм комп'ютерного зору в реальному часі, включаючи розпізнавання облич. Хоча сам OpenCV не надає моделей нейронних мереж, його можна інтегрувати з фреймворками глибокого навчання, такими як TensorFlow, PyTorch або Dlib, для створення надійної системи розпізнавання облич. Огляд розпізнавання обличчя
Розпізнавання обличчя – це багатоетапний процес, який включає розпізнавання обличчя, виділення ознак і ідентифікацію обличчя. Система спочатку визначає наявність облич у кадрі зображення чи відео. Після виявлення облич система виділяє унікальні характеристики з кожного обличчя, які потім використовуються для ідентифікації або верифікації особи. Розпізнавання обличчя є початковим і вирішальним кроком у системі розпізнавання обличчя. Цей крок передбачає визначення облич у кадрі зображення чи відео. OpenCV пропонує кілька попередньо підготовлених класифікаторів для виявлення облич, таких як каскади Хаара та підхід Гістограма орієнтованих градієнтів (HOG) + опорна векторна машина (SVM). Однак більш сучасні та точні методи використовують моделі глибокого навчання. Каскади Хаара є одним із найстаріших методів визначення обличчя. Вони працюють, застосовуючи серію згорткових фільтрів до зображення, щоб виявити різні риси обличчя, як-от краї, текстури та форми. Незважаючи на те, що каскади Хаара є швидкими та ефективними, вони часто страждають від нижчої точності та вищих показників помилкових позитивних результатів порівняно з сучасними методами. Dlib забезпечує більш точний детектор обличчя на основі згорткової нейронної мережі (CNN). Цей метод забезпечує кращу продуктивність у різних умовах, наприклад під різним освітленням, кутами та оклюзіями. Детектор обличчя CNN сканує зображення та визначає області, які ймовірно містять обличчя. Після виявлення

облич наступним кроком є виділення відмінних рис кожного обличчя. Ці риси мають бути унікальними для кожної людини та стійкими до варіацій пози, виразу та освітлення. Моделі глибокого навчання, зокрема згорткові нейронні мережі (CNN), відмінно справляються з цим завданням. Деякі популярні моделі для виділення ознак обличчя включають FaceNet, VGG-Face і модель розпізнавання обличчя на основі ResNet Dlib. FaceNet, розроблений Google, використовує глибоку згортку для відображення облич у 128-вимірному просторі вбудовування. У цьому просторі евклідова відстань між двома вкладеннями граней відповідає подібності між гранями. FaceNet було навчено з використанням великого набору даних зображень облич і може створювати високорозбірливі вбудовування облич. VGG-Face — ще одна популярна модель для розпізнавання осіб. Розроблено Visual Geometry Group в Оксфордському університеті, воно базується на архітектурі VGG-16. VGG-Face навчено розпізнавати обличчя шляхом вивчення широкого набору функцій, які фіксують різні аспекти зовнішнього вигляду обличчя. Модель розпізнавання облич Dlib базується на ResNet, глибокій залишковій мережі. Ця модель генерує 128-вимірний вектор (вбудовування) для кожного обличчя, фіксуючи унікальні риси обличчя. Архітектура ResNet дозволяє ефективно навчати глибокі мережі за допомогою залишкових з’єднань, які допомагають пом’якшити проблему зникнення градієнта. За допомогою витягнутих вбудовувань можна виконати розпізнавання облич, порівнюючи вбудовування виявлених облич із тими, що містяться в базі даних відомих облич. Цей процес зазвичай передбачає використання метрики відстані, наприклад евклідової відстані або класифікатора машинного навчання. Простим і ефективним підходом до розпізнавання обличчя є використання метрики відстані. Ідея полягає в тому, щоб порівняти вбудовування виявленого обличчя з вбудовуванням відомих облич. Якщо відстань між вкладеннями нижче певного порогу, обличчя вважається збігом. Для більш надійного розпізнавання можна використовувати класифікатори машинного навчання, такі як опорні векторні машини (SVM), k-Nearest Neighbors (k-NN) або навіть класифікатори глибокого навчання. Ці класифікатори навчаються на вбудованих гранях і

відповідних мітках (іменах). Під час висновку класифікатор передбачає мітку виявленого вбудовування обличчя. Перш ніж використовувати систему розпізнавання обличчя, класифікатор має бути навчений відомим вбудованим особам і відповідним міткам. Цей процес передбачає: Збір даних: збір набору даних зображень обличчя для кожної особи, яку потрібно розпізнати. Набір даних має містити кілька зображень кожної людини в різних умовах, щоб забезпечити надійність. Розпізнавання обличчя: визначення облич на кожному зображенні та виділення областей обличчя. Вилучення функцій: використання попередньо навченої моделі для вилучення вбудованих областей обличчя. Навчання: навчання класифікатора (наприклад, SVM, k-NN) на витягнутих вбудовуваннях та їхніх відповідних мітках. Реалізація з OpenCV і Deep Learning Щоб реалізувати систему розпізнавання обличчя за допомогою OpenCV і глибокого навчання, потрібно виконати наступні кроки: Ініціалізація моделей: завантаження моделі виявлення обличчя та моделі розпізнавання обличчя. Для визначення обличчя можна використовувати детектор на основі CNN. Для розпізнавання обличчя можна використовувати попередньо навчену модель, наприклад FaceNet або модель Dlib на основі ResNet. Захоплення відео: використовуйте OpenCV для захоплення відеокадрів із камери. Кожен кадр оброблятиметься для виявлення та розпізнавання облич у реальному часі. Розпізнавання обличчя: для кожного кадру виявляйте обличчя за допомогою моделі розпізнавання обличчя. Це передбачає перетворення кадру в градації сірого (якщо потрібно) і пропускання його через детектор. Вилучення функцій: для кожного виявленого обличчя витягніть область обличчя та використовуйте модель розпізнавання обличчя, щоб обчислити вбудовування обличчя. Розпізнавання обличчя: порівняйте обчислене вбудовування з вбудовуваннями в базі даних за допомогою метрики відстані або навченого класифікатора для розпізнавання обличчя. Відображення результатів: намалюйте рамки навколо виявлених облич і відобразіть імена та показники достовірності на відеокадрі. Сучасні моделі глибокого навчання забезпечують високу точність розпізнавання обличчя навіть у складних умовах. Надійність: моделі глибокого навчання стійкі до змін освітлення, пози та виразу обличчя.

Обробка в режимі реального часу: завдяки ефективному застосуванню системи розпізнавання облич можуть працювати в режимі реального часу, що робить їх придатними для таких програм, як безпека та спостереження. Обчислювальні ресурси. Моделі глибокого навчання потребують значних обчислювальних ресурсів, особливо для обробки в реальному часі. Конфіденційність даних: обробка даних про обличчя викликає занепокоєння щодо конфіденційності. Необхідно вжити належних заходів для забезпечення безпеки та конфіденційності даних. Зміщення набору даних: на продуктивність моделей розпізнавання облич можуть впливати зміщення в наборі навчальних даних. Для навчання моделей важливо використовувати різноманітний і репрезентативний набір даних. Безпека та спостереження: автоматизовані системи безпеки використовують розпізнавання облич, щоб ідентифікувати людей у режимі реального часу, підвищуючи безпеку в громадських і приватних місцях.

Контроль доступу: розпізнавання обличчя використовується в системах контролю доступу для автентифікації осіб і надання доступу до безпечних зон.

Персональні пристрої: смартфони та ноутбуки використовують розпізнавання обличчя для автентифікації користувачів, забезпечуючи зручний і безпечний спосіб розблокування пристроїв. Взаємодія з клієнтами. У галузях роздрібної торгівлі та гостинності розпізнавання облич використовується для персоналізації взаємодії з клієнтами, наприклад для надання індивідуальних рекомендацій і послуг. Майбутнє технології розпізнавання облич, ймовірно, побачить подальший прогрес у точності, швидкості та надійності. Тривають дослідження для розробки більш ефективних моделей, які можуть працювати на малопотужних пристроях, таких як смартфони та вбудовані системи. Крім того, докладаються зусилля для вирішення проблем етики та конфіденційності, пов’язаних із технологією розпізнавання обличчя.

3.2 Розробка Dataset

```
import cv2
import os

cam = cv2.VideoCapture(0)
cam.set(3, 640) # set video width
cam.set(4, 480) # set video heigh

face_detector = cv2.CascadeClassifier('faces_model.xml')

face_id = input('\n enter user id end press <return> ==>  ')

print("\n [INFO] Initializing face capture. Look the camera and wait ...")
count = 0
REQUIRED_COUNT = 200
```

Імпортуються бібліотеки cv2 та os.

cv2 – це і є бібліотека computer vision.

os – бібліотека яка допомагає взаємодіїти з операційною системою й файлами.

cv2.VideoCapture(0) ініціалізує веб-камеру. 0 означає, що використовується доступна перша камера.

cam.set(3, 640) і cam.set(4, 480) встановлюють ширину та висоту відео відповідно.

Завантаження моделі для розпізнавання облич:

face_detector = cv2.CascadeClassifier('faces_model.xml')

Завантажується модель розпізнавання облич CascadeClassifier, використовуючи файл faces_model.xml.

Запит ідентифікатора користувача:

face_id = input('\n enter user id and press <return> ==> ')

Програма запитує користувача ввести ідентифікатор, який буде використовуватися для іменування файлів зображень.

Початок захоплення зображень:

print("\n [INFO] Initializing face capture. Look at the camera and wait ...")

count = 0

REQUIRED_COUNT = 200

Друкується повідомлення користувача. Ініціалізується лічильник count, який відстежує кількість збережених зображень.

REQUIRED_COUNT задає потрібну кількість зображень, які потрібно захопити (200).

```
while(True):

    ret, img = cam.read()
    gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
    faces = face_detector.detectMultiScale(gray, 1.3, 5)

    for (x,y,w,h) in faces:
        print(x,y,w,h)
        cv2.rectangle(img, (x,y), (x+w,y+h), (255,0,0), 2)
        count += 1

        cv2.imwrite("dataset/User." + str(face_id) + '.' + str(count) + ".jpg",
gray[y:y+h,x:x+w])

        cv2.imshow('image', img)

    k = cv2.waitKey(100) & 0xff
    if k == 27:
        break
    elif count >= REQUIRED_COUNT:
         break
```

Основний цикл захоплення зображень:

У нескінченному циклі виконується захоплення зображення з камери.

Зображення конвертується у відтінки сірого для покращення роботи алгоритму розпізнавання облич.

detectMultiScale виявляє обличчя на зображенні.

Для кожної виявленої особи:

Координати обличчя відображаються на екрані.

Малюється прямокутник навколо обличчя зображення.

Збільшується лічильник count.

Зображення обличчя зберігається в папці dataset з ім'ям User.<face_id>.<count>.jpg.

Показ зображення з намальованим прямокутником навколо обличчя.

Якщо натиснути клавішу ESC (код 27), програма завершує роботу.

Якщо кількість збережених зображень досягла REQUIRED_COUNT, програма також завершує роботу.

```
print("\n [INFO] Exiting Program and cleanup stuff")
cam.release()
cv2.destroyAllWindows()
```

Друкується повідомлення про завершення роботи програми. Вивільняються ресурси, пов'язані з камерою. Закриваються усі вікна OpenCV. Таким чином, цей скрипт захоплює 200 зображень осіб користувача з веб-камери, обробляє їх для розпізнавання облич та зберігає результати в папку dataset.

3.3. Розробка тренувального коду для computer vision

```
import cv2
import numpy as np
from PIL import Image
import os

path = 'dataset'

recognizer = cv2.face.LBPHFaceRecognizer_create()
detector = cv2.CascadeClassifier("faces_model.xml");
```

cv2: Бібліотека OpenCV використовується для обробки зображень та відео.

numpy: Бібліотека для роботи із масивами.

PIL (Pillow): Бібліотека для обробки зображень.

os: Модуль для роботи з файловою системою.

path: Шлях до папки, де зберігаються зображення облич.

Створення об'єкта розпізнавання облич та завантаження моделі розпізнавання облич.

recognizer: Створення об'єкта розпізнавача осіб за допомогою методу LBPH.

detector: Створення об'єкта детектора осіб за допомогою каскадного класифікатора, завантажуваного з файлу faces_model.xml.

```
def getImagesAndLabels(path):

    imagePaths = [os.path.join(path,f) for f in os.listdir(path)]
    faceSamples=[]
    ids = []

    for imagePath in imagePaths:

        PIL_img = Image.open(imagePath).convert('L')
        img_numpy = np.array(PIL_img,'uint8')

        id = int(os.path.split(imagePath)[-1].split(".")[1])
        faces = detector.detectMultiScale(img_numpy)

        for (x,y,w,h) in faces:
            faceSamples.append(img_numpy[y:y+h,x:x+w])
            ids.append(id)

    return faceSamples,ids
```

imagePaths: Список шляхів до всіх файлів у папці dataset.

faceSamples: Список для зберігання вирізаних облич із зображень.

ids: Список для зберігання ідентифікаторів осіб, які витягли з імен файлів.

PIL_img: Відкриття зображення за допомогою PIL та перетворення його на відтінки сірого.

img_numpy: Перетворення зображення на масив NumPy з типом даних uint8.

id: Вилучення ідентифікатора особи з імені файлу. Передбачається, що імена файлів мають формат User.<id>.<номер>.jpg.

faces: Список координат прямокутників, що охоплюють кожну виявлену особу.

Вирізання обличчя із зображення та додавання його до списку faceSamples.

Додавання відповідного ідентифікатора до списку ID.

```
print ("\n [INFO] Training faces. It will take a few seconds. Wait ...")
faces,ids = getImagesAndLabels(path)
recognizer.train(faces, np.array(ids))

recognizer.write('trainer/trainer.yml')
print("\n [INFO] {0} faces trained. Exiting Program".format(len(np.unique(ids))))
```

Виведення повідомлення про початок процесу навчання.

Викликає функції getImagesAndLabels, щоб отримати зразки осіб та їх ідентифікатори.

Навчання моделі розпізнавання осіб із використанням методу train.

Збереження навченої моделі у файлі trainer.yml.

Виведення повідомлення про кількість навчених осіб.

Таким чином, цей код створює модель розпізнавання облич на основі зображень, що містяться у зазначеній папці, і зберігає навчену модель файлу.

3.4. Реалізація computer vision

```
import cv2
import numpy as np
import os

recognizer = cv2.face.LBPHFaceRecognizer_create()
recognizer.read('trainer/trainer.yml')
cascadePath = "faces_model.xml"
faceCascade = cv2.CascadeClassifier(cascadePath);

font = cv2.FONT_HERSHEY_SIMPLEX
```

recognizer: Створення об'єкта розпізнавача осіб із використанням методу LBPH та завантаження навченої моделі з файлу trainer.yml.

faceCascade: Створення об'єкта каскадного класифікатора для виявлення облич із використанням моделі з файлу faces_model.xml.

font: Вибір шрифту для відображення тексту на зображенні. ID: Ініціалізація ідентифікатора.

```
id = 0

names = ['None', 'Jora', 'Kirill']

cam = cv2.VideoCapture(0)
cam.set(3, 640)
cam.set(4, 480)

minW = 0.1*cam.get(3)
minH = 0.1*cam.get(4)
```

names: Список імен, які відповідають ідентифікаторам осіб.

cam: Ініціалізація захоплення відео із веб-камери.

Налаштування ширини та висоти відео.

minW та minH: Визначення мінімальних розмірів вікна для розпізнавання обличчя, що залежить від розмірів відео.

```
while True:

    ret, img =cam.read()
    gray = cv2.cvtColor(img,cv2.COLOR_BGR2GRAY)

    faces = faceCascade.detectMultiScale(
        gray,
        scaleFactor = 1.2,
        minNeighbors = 5,
        minSize = (int(minW), int(minH)),
       )

    for(x,y,w,h) in faces:

        cv2.rectangle(img, (x,y), (x+w,y+h), (0,255,0), 2)

        id, confidence = recognizer.predict(gray[y:y+h,x:x+w])

        # Check if confidence is less them 100 ==> "0" is perfect match
        print(confidence)
        if (confidence < 100):
            id = names[id]
            confidence = "  {0}%".format(round(100 - confidence))
        else:
            id = "unknown"
            confidence = "  {0}%".format(round(100 - confidence))

        cv2.putText(img, str(id), (x+5,y-5), font, 1, (255,255,255), 2)
        cv2.putText(img, str(confidence), (x+5,y+h-5), font, 1, (255,255,0), 1)
```

```
    cv2.imshow('camera',img)

    k = cv2.waitKey(10) & 0xff # Press 'ESC' for exiting video
    if k == 27:
        break
```

Цикл while True: Запускає нескінченний цикл, який продовжуватиметься доти, доки не буде виконана умова виходу.

cam.read(): Захоплює поточний кадр із веб-камери.

ret: Логічне значення, що вказує на успішність захоплення кадру.

img: Сам захоплений кадр.

cv2.cvtColor(img, cv2.COLOR_BGR2GRAY): Перетворює кольорове зображення (у форматі BGR) у відтінки сірого, оскільки алгоритми розпізнавання облич зазвичай працюють із чорно-білими зображеннями.

faceCascade.detectMultiScale: Виявляє обличчя на зображенні у відтінках сірого.

gray:

Вхідне зображення у відтінках сірого.

scaleFactor=1.2: Параметр, який визначає, наскільки зменшується зображення на кожному масштабі.

minNeighbors=5: Кількість сусідів кожного прямокутника-кандидата. Чим більше це значення, тим вища ймовірність того, що виявлений об'єкт – особа.

minSize=(int(minW), int(minH)): Мінімальний розмір об'єкта, який можна розпізнати як обличчя.

faces: Список координат прямокутників, що охоплюють кожну виявлену особу. Кожен елемент списку містить координати верхнього лівого кута та розміри прямокутника: (x, y, w, h).

Цикл for (x, y, w, h) in faces: Обробляє кожну виявлену особу.

cv2.rectangle(img, (x, y), (x+w, y+h), (0, 255, 0), 2): Малює прямокутник навколо виявленої особи.

(x, y): Координати верхнього лівого кута прямокутника.

(x+w, y+h): Координати правого нижнього кута прямокутника.

(0, 255, 0): Колір прямокутника (зелений).

«2»: Товщина лінії прямокутника.

recognizer.predict(gray[y:y+h, x:x+w]): Розпізнає обличчя у вказаній області зображення.

gray[y:y+h, x:x+w]: Область зображення, що містить обличчя.

id: Ідентифікатор розпізнаної особи.

confidence: Рівень впевненості у розпізнаванні (чим менше значення, тим вища впевненість).

Перевірка рівня впевненості:

Якщо confidence < 100: Розпізнавання успішно, надається ім'я, відповідне id.

Якщо confidence >= 100: Особа не розпізнана, надається ім'я "unknown".

cv2.imshow('camera', img): Відображає поточний кадр у вікні під назвою 'camera'.

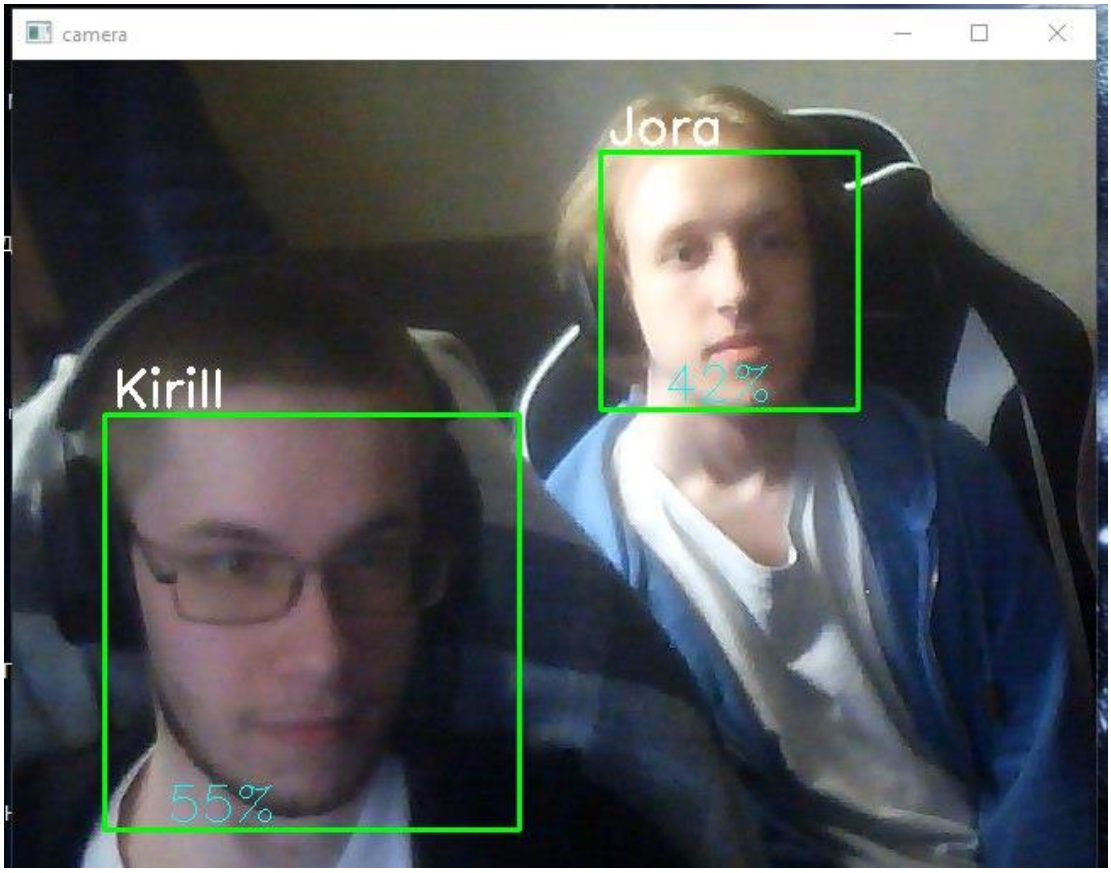
cv2.waitKey(10) & 0xff: Очікування натискання клавіші протягом 10 мілісекунд. Якщо натиснути клавішу ESC (код 27), цикл переривається і програма завершується.

cam.release(): Звільняє захоплені ресурси камери.

cv2.destroyAllWindows(): Закриває всі вікна OpenCV.

```
print("\n [INFO] Exiting Program and cleanup stuff")
cam.release()
cv2.destroyAllWindows()
```

Таким чином, цей код захоплює відеопотік з веб-камери, виявляє обличчя, розпізнає їх за допомогою попередньо навченої моделі та відображає результати в реальному часі.



Як бачите computer vision працює справно й показує що код натренерованний і розпізнає обличчя людей що знаходятся в базі данних

ВИСНОВКИ

Технологія комп’ютерного бачення стала кардинальною для покращення можливостей моніторингу та безпеки корпоративних середовищ. Використовуючи складні алгоритми аналізу зображень і відео, організації тепер можуть виявляти загрози безпеці та реагувати на них у режимі реального часу, започатковуючи проактивну парадигму керування мережевою безпекою. Однією з ключових переваг інтеграції технології комп’ютерного зору є її здатність використовувати існуючу інфраструктуру відеоспостереження, мінімізуючи потребу у дорогих інвестиціях у апаратне забезпечення. Цей економічно ефективний підхід не тільки оптимізує використання ресурсів, але й спрощує процес розгортання, забезпечуючи плавний перехід до розширених заходів безпеки. Крім того, впровадження технології комп’ютерного зору значно зменшує залежність від традиційних засобів фізичної безпеки, таких як пілотовані патрулі або статичні системи відеоспостереження. Завдяки автоматизації завдань спостереження та інтелектуальному виявленню загроз підприємства можуть досягти вищого рівня безпеки, мінімізуючи операційні витрати. Іншим переконливим аспектом технології комп’ютерного зору є її масштабованість і адаптованість до різноманітних корпоративних середовищ. Незалежно від того, чи це невеликий стартап, чи транснаціональна корпорація, організації можуть адаптувати рішення комп’ютерного бачення відповідно до своїх конкретних потреб безпеки, забезпечуючи тим самим комплексний захист від нових загроз. На додаток до посилення протоколів безпеки, технологія комп’ютерного зору також пропонує додаткові переваги, такі як підвищена операційна ефективність і можливості аналізу даних. Аналізуючи потоки візуальних даних, організації можуть отримати цінну інформацію про поведінку клієнтів, оптимізувати логістичні процеси та навіть покращити контроль якості продукції. По суті, технологія комп’ютерного зору є універсальним і незамінним інструментом для сучасних підприємств, які прагнуть зміцнити свою безпеку.

Використовуючи цю інноваційну технологію, організації можуть не лише захистити свої активи та персонал, але й відкрити нові шляхи для зростання та інновацій у світі, що стає все більш цифровим.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Особливості побудови і використання сучасних корпоративних комп'ютерних мереж - 2017 - Режим доступу: https://conferences.vntu.edu.ua/public/files/1/fitki_2017_netpub.pd

2. Як не заплутатися у дротах. Типи мережевих кабелів – 2023 - Режим доступу: https://maxnet.ua/blog/kak-ne-zaputatsya-v-provodakh-tipy-setevykh-kabeley/

3. Cisco AVVID Network Infrastructure Overview доступу до ресурсу: https://www.cisco.com/web/offer/CAT4500/toolkit/comin_ov.pdf

4. Побудова корпоративних мереж передачі даних - 2019 - Режим доступу: https://www.telesphera.net/blog/corporate-networking.html

5. Особливості побудови і використання сучасних корпоративних комп'ютерних мереж - 2017 - Режим доступу: https://conferences.vntu.edu.ua/public/files/1/fitki_2017_netpub.pdf

6. База даних OpenCV з натренерованими нейроними мережами: https://opencv.org/releases/

7. Asterisk ConfBridge режим доступу до ресурсу: https://wiki.asterisk.org/wiki/display/AST/ConfBridge

8. Загальні принципи побудови корпоративної мережі - 2020 Режим доступу: - https://studfile.net/preview/5470625/

9. Як не заплутатися у дротах. Типи мережевих кабелів – 2023 - Режим доступу: https://maxnet.ua/blog/kak-ne-zaputatsya-v-provodakh-tipy-setevykhkabeley/

10. Cybersecurity, everywhere you need it - 2023 - Режим доступу: https://www.fortinet.com/

11. Gigabit Ethernet - 2016 - Режим доступу: https://wiki.cuspu.edu.ua/index.php/Gigabit_Ethernet

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

на тему: «Удосконалення засобів захисту корпоративних комп'ютерних мереж за допомогою технології computer vision»

Виконав студент групи КІД-42
Будкін Кирило Павлович

Керівник кваліфікаційної роботи:
Лемешко Андрій Вікторович,
Доцент кафедри КІ

Київ – 2024

Мета роботи - дослідження та розробка інноваційних методів для підвищення безпеки корпоративних комп'ютерних мереж шляхом використання технологій computer vision.

Об'єкт дослідження - інфраструктура корпоративної комп'ютерної мережі з computer vision.

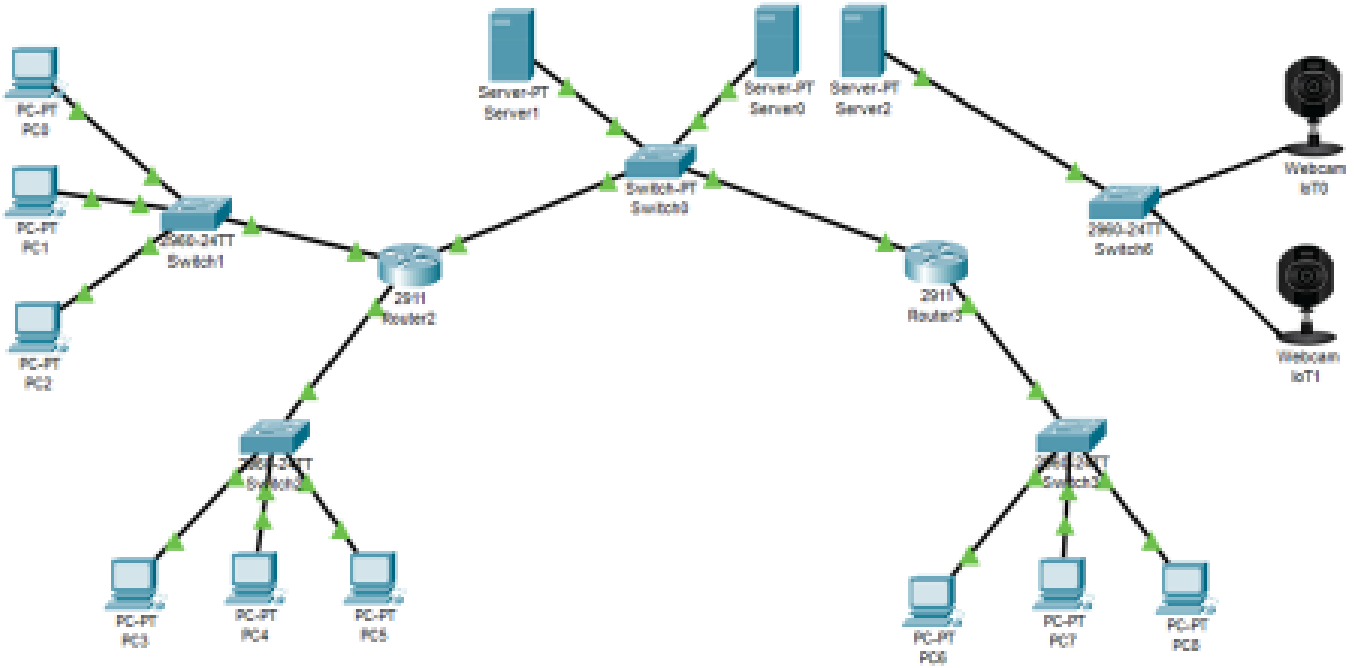
Предмет дослідження - застосування технологій computer vision в контексті кібербезпеки.

2

Актуальність обраної теми

Актуальність досліджуваної проблеми полягає в тому, що з розвитком конкуренції значного поширення набули такі злочини, як викрадання інформації через комп'ютерні мережі і прослуховування ліній зв'язку. З ростом кіберзагроз, які стають все більш складними та вдосконаленими завдяки розвитку технологій, важливо постійно удосконалювати методи захисту. Використання технології computer vision в цьому контексті може допомогти виявляти нові методи атак та забезпечувати більш ефективну захист корпоративних мереж.

Корпоративна мережа



Реалізація таких протоколів як:

DHCP
DNS
TCP
UDP
SNMP
ICMP
IPSec
NFS

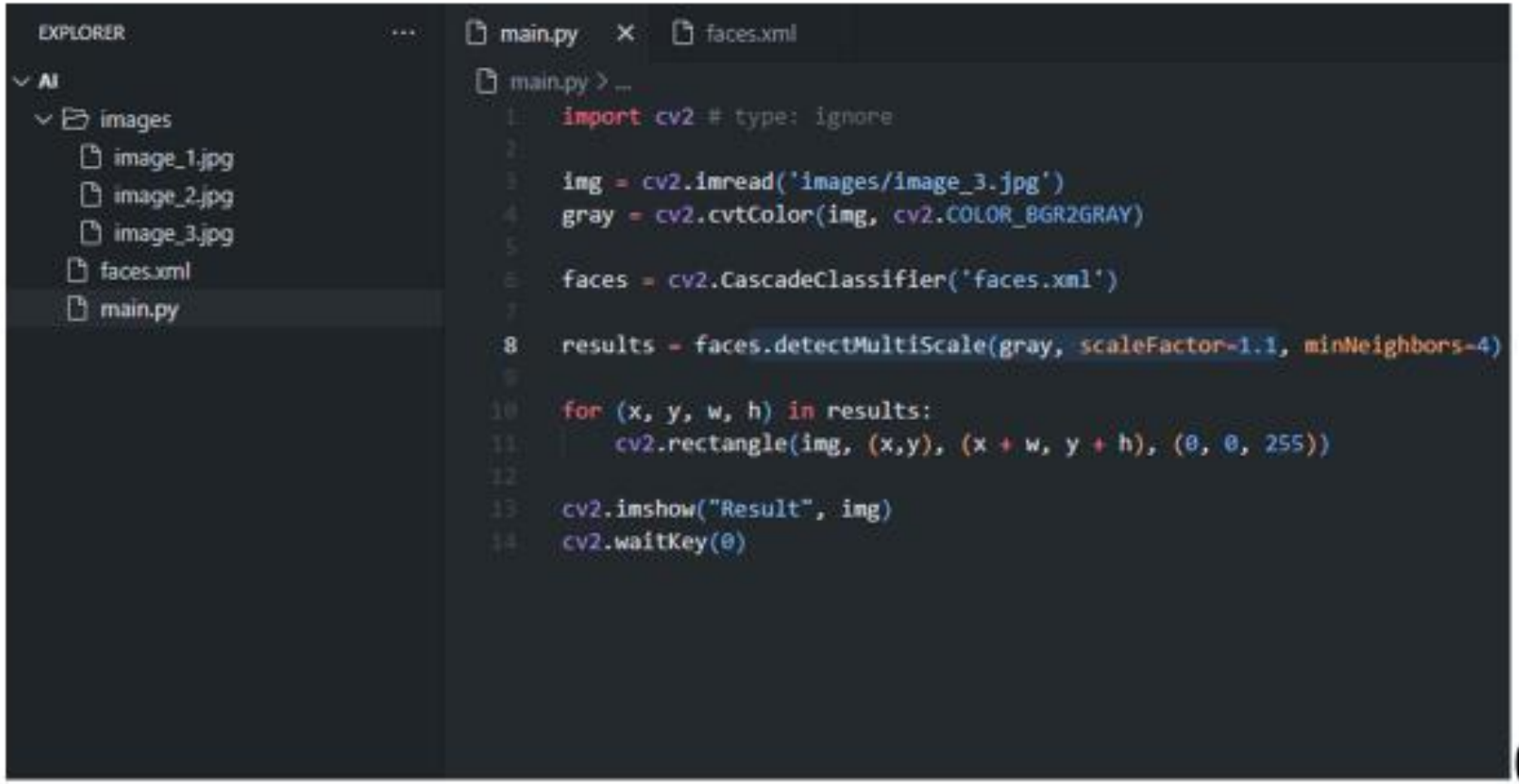
4

Computer Vision

Computer Vision — це галузь технологій, яка дозволяє комп'ютерам бачити, інтерпретувати та розуміти візуальну інформацію з навколишнього світу.

5

Код розпізнавання обличчя на зображенні

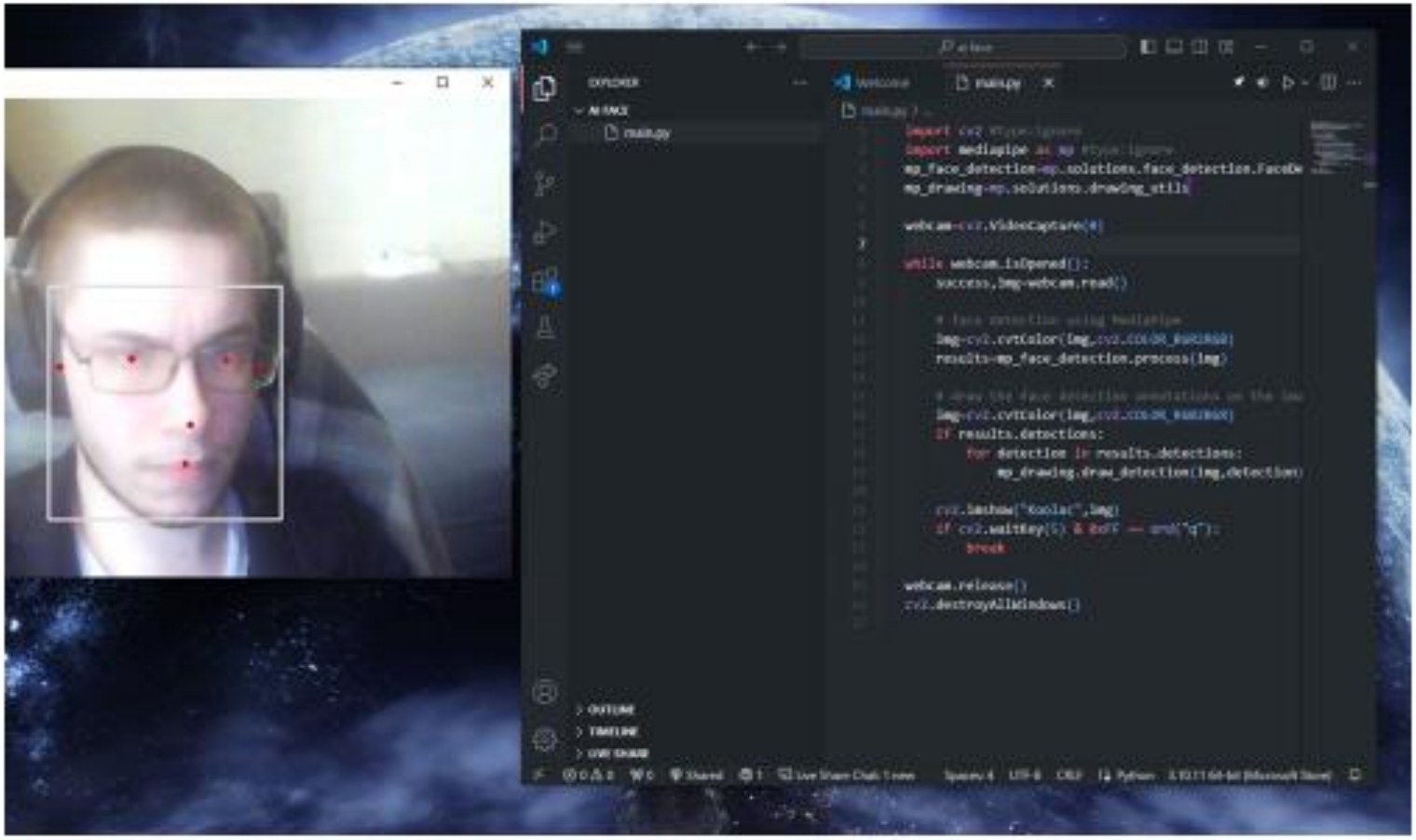


6

Результат коду розпізнавання обличчя на зображенні

7

Написання коду що розпізнає обличчя з відео камери

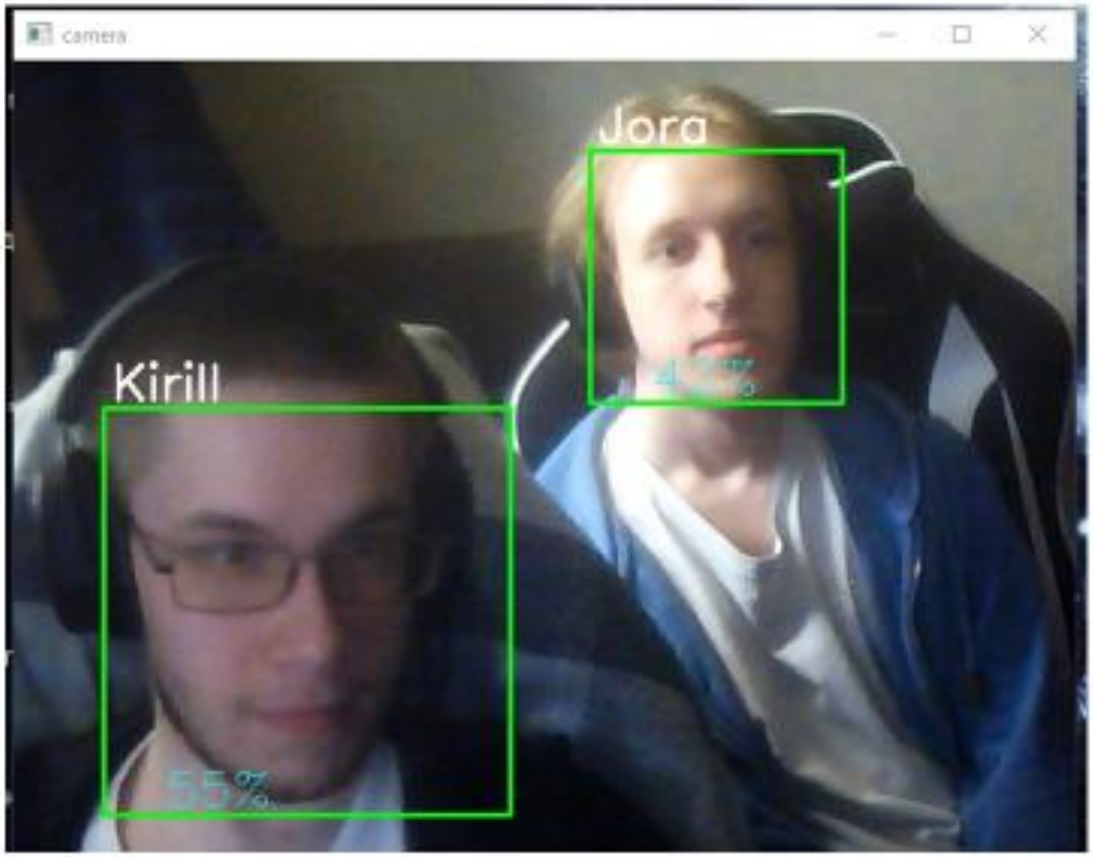


8

Реалізація коду с розпізнаванням людей

```python
import cv2
import numpy as np
from PIL import Image
import os

# Path for face image database
path = 'dataset'

recognizer = cv2.face.LBPHFaceRecognizer_create()
detector = cv2.CascadeClassifier("Faces_model.xml");

# function to get the images and label data
def getImagesAndLabels(path):

    imagePaths = [os.path.join(path,f) for f in os.listdir(path)]
    faceSamples=[]
    ids = []

    for imagePath in imagePaths:

        PIL_img = Image.open(imagePath).convert('L') # convert it to grayscale
        img_numpy = np.array(PIL_img,'uint8')

        id = int(os.path.split(imagePath)[-1].split(".")[1])
        faces = detector.detectMultiScale(img_numpy)

        for (x,y,w,h) in faces:
            faceSamples.append(img_numpy[y:y+h,x:x+w])
            ids.append(id)

    return faceSamples,ids

print ("\n [INFO] Training faces. It will take a few seconds. Wait ...")
faces,ids = getImagesAndLabels(path)
recognizer.train(faces, np.array(ids))

# Save the model into trainer/trainer.yml
recognizer.write('trainer/trainer.yml') # recognizer.save() worked on Mac, but not on Pi

# Print the number of faces trained and end program
print("\n [INFO] {0} Faces trained. Exiting Program".format(len(np.unique(ids))))
```

Результат



10

ВИСНОВКИ

Технологія комп'ютерного бачення значно покращує можливості моніторингу та безпеки корпоративного середовища. Використовуючи вдосконалений аналіз зображень і відео, організації можуть виявляти загрози та реагувати на них у режимі реального часу, забезпечуючи активний підхід до безпеки мережі. Використання існуючої інфраструктури відеоспостереження та інтеграція технології комп'ютерного зору може бути економічно ефективним рішенням для підвищення безпеки. Це зменшує потребу в додаткових заходах фізичної безпеки та використовує вже наявні ресурси. Технологія комп'ютерного бачення є високомасштабованою та адаптованою до різних корпоративних середовищ. Його можна налаштувати відповідно до конкретних потреб безпеки, що робить його універсальним рішенням для різних галузей промисловості та організаційного розміру.

11