DOI: 10.25140/2411-5363-2023-1(31)-80-89
УДК 004.056.5

Микола Гумен[1], Дмитро Кущевський[2]

[1]кандидат технічних наук, доцент, заступник декана факультету аеронавігації, електроніки та телекомунікацій
Національний авіаційний університет (Київ, Україна)
E-mail: mbgumen@ukr.net. **ORCID:** https://orcid.org/0000-0001-7935-6496

[2]студент освітнього ступеня магістр
Національний авіаційний університет (Київ, Україна)
E-mail: dima.kushhevskij@gmail.com

СИСТЕМА ВИЯВЛЕННЯ ПРОНИКНЕНЬ НА БАЗІ UWB-ТЕХНОЛОГІЇ

Розглянуто та проаналізовано системи контролю доступу персоналу для забезпечення захисту від зовнішніх та внутрішніх правопорушників. Розроблено систему виявлення сторонніх осіб у приміщеннях установ та організацій Проаналізовано стандарти RFID, BLE, WiFi, UWB та актуальність їх застосування в запропонованій системі. Для реалізації в системі обрано стандарт бездротового зв'язку UWB (802.15.4z). Система дає змогу ідентифікувати уповноважених працівників та виявляти зловмисників у реальному часі без розпізнавання облич та складних алгоритмів машинного навчання.

Ключові слова: *система контролю доступу, виявлення проникнень, зловмисник, анкор, тег, надширокосмугова технологія, комп'ютерний зір, згорткова нейронна мережа, бездротова технологія.*

Табл.: 4. Рис.: 4. Бібл.: 15.

Актуальність теми дослідження. В умовах стрімкого впровадження бездротової передачі інформації та жорсткої конкурентної боротьби на ринку інформаційних технологій дотримання умов секретності та протидії витоку інформації актуальною є проблема забезпечення контрольованого доступу до обладнання та приміщень об'єктів різноманітного призначення.

На сьогодні системи контролю та управління доступом, різні за об'ємом функціонала та складністю, дедалі більше застосовуються в навчальних (університет, школа, дитячий садок), робочих (офіси, коворкінг), промислових (фабрики, заводи) установах та організаціях. Такі системи дають змогу в реальному часі фіксувати та реєструвати пересування осіб, а також реагувати на випадки неправомірного проникнення.

Не менш важливим є завдання виявлення правопорушників. Безумовно, чим більший штат установи, тим легше злочинцю перебувати всередині та виконувати задумане. Так, можливість мати фізичний доступ до каналів зв'язку та комп'ютерів спричинює цілий спектр загроз, починаючи від фізичної крадіжки обладнання та закінчуючи компрометацією установ та організацій.

Постановка проблеми. Більшість установ та організацій мають просту систему авторизації, яка містить пасивну RFID (Radio Frequency IDentification – радіочастотна ідентифікація) карту та камери, за якими слідкує оператор. Пасивні RFID карти являють собою крихітний радіоприймач, якому для активації та передачі сигналу відповіді достатньо потужності магнітного поля. При спрацьовуванні електромагнітним імпульсом опитування від найближчого пристрою зчитування RFID тег передає у зворотному напрямку до зчитувача цифрові дані, зазвичай ідентифікаційний номер. Цю технологію використовують у таких системах контролю доступу, як турнікети, двері з магнітним замком тощо.

Системи подібного типу мають багато недоліків, спричинених якістю карт, їхньою стійкістю до підробки, людським фактором (охороною на вході до об'єкта та персоналом, який контролює камери).

Людський фактор доволі просто дає змогу зловмисникам спочатку, проаналізувавши роботу компанії або підприємства, вивчити поведінку співробітників, а потім, використовуючи техніки соціальної інженерії та технічні засоби, потрапити в будівлю.

Рішення, які є на ринку, наприклад, AJAX StarterKit Cam Plus, AJAX DualCurtain Outdoor та інші, націлені на захист від втручання в той час, коли офіс зачинений, але

вони не здатні ідентифікувати зловмисника в робочий час, що створює прогалину в системі безпеки. Використання розпізнавання облич для вирішення цього завдання не завжди є достатньо ефективним, бо потребує хорошої якості камер або їх великої кількості, спеціалізованого програмного забезпечення та ускладнює процес прийому і звільнення співробітників [1].

Аналіз останніх досліджень та публікацій. Серед останніх досліджень можна виділити такі, що спрямовані на оптимізацію використовуваних протоколів та технологій [2]. Результати зазначених досліджень дають змогу покращити показники енергоспоживання та стабільності датчиків, які гарно підходять для осель, але вони не вирішують проблему проникнення в установи й зорієнтовані на примітивні системи детектування відривання дверей, вікон та руху в приміщенні. Також є рішення, які реалізують нові підходи [3], а саме використання пасивних інфрачервоних датчиків (PIR) для виявлення руху та алгоритми комп'ютерного зору. Такі рішення хоч і є доповненням до існуючих систем захисту від проникнень, але вони зберігають головний недолік, а саме неможливість роботи у приміщеннях, де є авторизовані та неавторизовані особи.

Виділення недосліджених частин загальної проблеми. У наявних дослідженнях та публікаціях мало приділено уваги системам контролю та управління доступом, які дають змогу в реальному часу ідентифікувати працівників установ та організацій та виявляти зловмисників у приміщеннях на базі алгоритмів без розпізнавання облич.

Метою статті є розробка системи автоматичної ідентифікації людей у приміщенні без розпізнавання облич на основі бездротових технологій і алгоритмів комп'ютерного зору.

Виклад основного матеріалу. Розроблена система виявлення проникнень на базі алгоритмів комп'ютерного зору та бездротової UWB (Ultra-Wide Band – ультраширокий діапазон) технології складається зі стереокамер із вбудованими в них чипами, що підтримують UWB стандарт (далі – анкори), бездротових UWB девайсів, керуючого сервера та програмного забезпечення (ПЗ).

Запропонована реалізація системи потребує вирішення таких завдань: визначити кількість людей у кімнаті, виміряти відстань від камери до кожної особи, виявити порушника та створити повідомлення для відділу безпекової діяльності установи. Ясна річ, що чим більше камер ми будемо використовувати, тим точніше можна визначити кількість та позицію осіб у приміщенні, а отже, більш надійною буде система.

Для зрозумілого опису системи обираємо приміщення прямокутної форми, у якій можуть знаходитися чотири особи, три з яких є співробітниками установи, а одна особа є зловмисником. Будемо вважати, що приблизна площа на одну особу становить 7,5 м^2. Тоді довжина кімнати може дорівнювати 5 м, ширина 6 м, а висота 3 м.

Освітленість приміщення повинна забезпечити адекватне функціонування відеообладнання і бути не меншою за допустиме середнє значення освітленості, яке, зазвичай, становить 300 люкс. Додаткові предмети в приміщенні відсутні, зважаючи на те, що в кімнатах зловмисник не буде ховатись, оскільки це приверне увагу співробітників і приведе до його розкриття.

Для покриття простору, зменшення похибки розрахунку відстані від камер до особи та для демонстрації прийнятих рішень скористаємося трьома камерами.

Встановлено, що для виявлення обличчя людини на зображенні достатньо 4 пікселів (табл. 1). Оскільки обличчя дорослої людини становить $^1/_8$ частку від зображення його тіла, то мінімальний розмір людини на зображені повинен становити трохи більше за 32 пікселі.

З урахуванням зазначеного, а також заявлених вимог до параметрів кімнати, для яких найбільша відстань до об'єкта не перевищує 7…8 метрів, нам підходить більшість камер на ринку [4].

Таблиця 1 – Відношення якості картинки до точності обробки об'єктів

Вид операції	Допустимі значення		
	піксель/обличчя	піксель/см	піксель/дюйм
Ідентифікація (складні умови)	80	5	12,5
Ідентифікація (сприятливі умови)	40	2,5	6,3
Розпізнання	20	1,25	3,2
Детектування (виділення)	4	0,25	0,6

Джерело: розроблено авторами.

Вибір методів виділення об'єктів на зображенні та визначення відстані до них.

Для розрахунку відстані до людей необхідно виявити їх на зображенні камери та визначити координати обмежуючих прямокутників. Метод виділення об'єктів на вхідних зображеннях – це алгоритм чи нейронна мережа, які вирішують задачу знаходження об'єкта в кадрі відео (рис. 1). На сьогодні є низка найуживаніших методів, які застосовуються для вирішення цієї задачі.

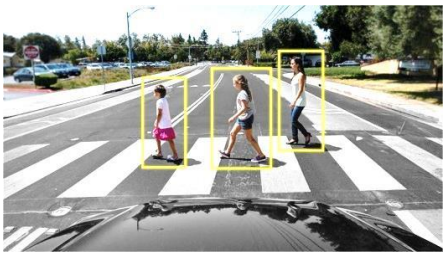

Рис. 1. Виділення об'єкта на зображенні

Джерело: розроблено авторами.

Алгоритм DPM (*Deformable Part Models*) ґрунтується на виявленні різних частин зображення та їх відносного положення для того, щоб потім визначити, чи є в кадрі об'єкт інтересу (зацікавленості) [5]. Так, наприклад, на основі певних ознак голови, рук, ніг, очей, торсу людини та за їхнім місцем положення на кадрі відео можна прийняти рішення про те, чи є на зображенні особа, для якої зазначені ознаки спрацьовують. Такий підхід дозволив побудувати модель, яка може працювати зі значною кількістю варіацій положень об'єктів, що виділяються.

Згорткова нейронна мережа R-CNN (Region Based Convolutional Neural Networks) [6]. Це одна з низки згорткових нейронних мереж (ЗНМ), використовуваних для розпізнавання конкретних образів на зображеннях, які подані масивами даних. У R-CNN реалізовано двоетапний алгоритм виділення об'єктів на основі регіональних зон інтересу. На початковому кроці двоетапного алгоритму ідентифікуються підмножини областей, які можуть містити об'єкт. На другому кроці класифікуються об'єкти цих областей.

Двоетапні алгоритми характеризуються дуже точними результатами розпізнавання об'єктів, однак за швидкодією поступаються одноетапним. Зумовлено це тим, що об'єкти можуть мати різні просторові розташування в межах зображення та різні співвідношення сторін обмежувальних прямокутників, а це потребує генерації величезної кількості областей інтересу.

Для мережі R-CNN кількість таких областей різних розмірів і співвідношень сторін не перевищує 2000, а їхнє формування здійснюється з використанням алгоритму вибіркового пошуку [6]. До характерних недоліків алгоритму належить його фіксованість, а отже, неможливість навчання мережі на початковому етапі та розв'язання задач розпізнавання об'єктів у режимі реального виміру часу.

Запропоновані пізніше ЗНМ Fast R-CNN та Faster R-CNN є більш швидкодіючими в порівнянні з базовою R-CNN мережею [7, 8]. При цьому швидкодія Faster R-CNN більша за швидкодію R-CNN у 245 разів, а Fast R-CNN у 11,5 раза, забезпечує можливість їхнього застосування для виявлення об'єктів у режимі реального часу.

You only look once (*YOLO*) є одноетапною ЗНМ архітектурою для виявлення об'єктів із повних зображень [9]. Модель працює за принципом розділення зображення на квадратні комірки, кожна з яких подається певною кількістю обмежувальних прямокутників. Далі для кожного обмежувального прямокутника мережа прогнозує ймовірність розта-

шування певного класу об’єкта. На завершальному етапі виділяються тільки ті прямокутники, в яких ймовірність розташування об’єкта вище за встановлене порогове значення. Точність застосування такого методу низька (особлива характерна помилка передбачення положення об’єкта), проте метод може обробляти від 45 кадрів відео в секунду та до 155 кадрів на секунду з оптимізованою моделлю.

Single Shot MultiBox Detector (SSMD) мережа запропонована в 2015 році [10]. Особливість моделі полягає у реалізації в ній трьох технік: одиничного проходу, мультибоксів, детектування. Техніка одиночного проходу забезпечує виокремлення областей інтересу та класифікація в один етап. Техніка мультибоксів дає змогу у фазі навчання сформувати області інтересу з фіксованими розмірами, за допомогою яких знаходяться об’єкти в режимі реального виконання, а техніка виявлення поєднує в собі одночасно і функціонал детектування та розпізнавання. Для оптимізації точності в моделі передбачено перевертання, обрізання та трансформація кольорів вхідного зображення.

EfficientDet. Сімейство ЗНМ EfficientDet є удосконаленням мережі EfficientNet [11] шляхом доповнення останньої шаром зі зваженою двонаправленою пірамідою ознак (BiFPN), що дає змогу легко і швидко об’єднувати багатомасштабні функції. На відміну від традиційних підходів у сімействі мереж EfficientDet реалізовано комплексний метод рівномірного та одночасного масштабування для всіх шарів мережі таких її параметрів, як *ширина, глибина та роздільна здатність, з фіксованим набором коефіцієнтів масштабування*». Практична реалізація зазначених методів забезпечила значне підвищення точності та ефективності сімейства мереж EfficientDet, а також зменшення на порядок вимог до значень параметрів та обчислювальних ресурсів порівняно з попередніми розробками ЗНМ.

CenterNet мережа на основі зображення генерує теплову карту, піки на якій відповідають центрам об’єктів. Розпізнавання образів на основі теплової карти можна, у деякому сенсі, розглядати як продовження одноетапного виявлення об'єктів. У той час як одноетапні алгоритми реалізують безпосереднє визначення координат прогнозованого обмежувального прямокутника, виявлення об’єктів за тепловою картою здійснюється на основі розподілу ймовірностей їх кутів або центрів. Розміщення цих кутових/центральних піків на теплових картах і визначає обмежувальні прямокутники. За швидкодією відповідні алгоритми все ще поступаються класичним одноетапним алгоритмам виявлення об’єктів.

На підставі аналізу особливостей методів виявлення об’єктів на зображеннях та даних табл. 2 в розробленій системі використана натренована модель на COCO 2017 ssd_mobilenet_v3, яка реалізована у фреймворку tensorflow.

Таблиця 2 – Порівняльна характеристика алгоритмів виявлення людей на зображенні

Показник	YOLOv4	SSMD	EfficientDet-D7x	CenterNet HarDNet-85	DPM	R-CNN
Швидкість обробки, кадр/секунда	45	59	30	45	4	5
Середня точність, %	63,4	74,3	55,1	43	41,9	65
Обробка в режимі реального часу	Так	Так	Ні	Так	Ні	Ні

Джерело: розроблено авторами.

Отримавши картинку з обведеними людьми, нам необхідно визначити відносну відстань до кожної особи. Забезпечити достатню точність результату можна як апаратними, так і програмними засобами. Серед апаратних рішень доцільним є використання стереокамери замість звичайної з одним об’єктивом [12].

Більшість програмних алгоритмів оцінки відстані потребують даних про реальний зріст особи, що не є можливим у цій ситуації. Використання певного середнього значення може привести до значних похибок. Достатню точність оцінки відстані на основі зображень дає алгоритм SSD (Sum of squared difference) [13] (табл. 3).

Таблиця 3 – Результати вимірювання за допомогою стереокамери та алгоритму SSD

Реальна відстань, м	**0,5**	**1**	**1,5**	**2**	**2,5**	**3**	**3,5**	**4**	**4,5**	**5**
Розрахована відстань, м	0,51	1,03	1,55	2,09	2,63	3,17	3,7	4,24	4,8	5,37
Похибка, см	0,1	0,3	0,5	0,9	0,3	1,7	2	2,4	3,0	3,7

Джерело: розроблено авторами.

Обґрунтування технології виявлення зловмисників.

За оцінками відстані на основі зображення можемо ідентифікувати всіх людей у приміщенні. Наступним кроком буде ідентифікація у приміщенні тільки співробітників та визначення їх просторових координат (задача позиціонування). Із цією метою на стереокамері, як зазначалось раніше, встановлюється UWB чіп, а кожний співробітник отримує UWB тег. У зловмисника такий тег відсутній.

Підробка або копіювання тега є дуже складним завданням. При виборі тегів ми орієнтуємось як на ергономічні, так і певні технічні рішення, зокрема тег не повинен спричиняти дискомфорт, а отже, бути компактним, стійким до впливу завад, забезпечувати достатньо високу точність результату та мінімально можливо енергоспоживання.

Для вирішення вищезазначеного завдання застосовуються та інші методи, зокрема зорієнтовані на ультразвукові технології [14]. Проте для офісів – це не найкращий вибір, оскільки загасання ультразвукових хвиль при проходженні через об’єкти є значним.

Дані для порівняння використовуваних сучасних бездротових технологій наведені в табл. 4.

Таблиця 4 – Порівняння бездротових технологій

Показник	**UWB**	**Bluetooth**	**WiFi**	**RFID**	**GPS**
Місце експлуатації (Б- будівля, В -вулиця)	Б, В	Б, В	Б, В	Б, В	В
Точність, м	0.1	1…5 м	5…15 м	0.3…1 м	5…20 м
Зона покриття	70…250 м	15…100 м	50…150 м	1…5 м	-
Захищеність за 5 бальною шкалою	5	2	2	2	3
Споживання енергії в режимах передавання (ТХ) та приймання (RX)	5 ндж ТХ 9 ндж RX	15 ндж ТХ 15 ндж RX	50 ндж ТХ 50 ндж RX	>50 ндж	>50 ндж

Джерело: розроблено авторами.

Зазначимо, що головним недоліком систем позиціонування на основі технологій Wi-Fi та Bluetooth є використання відношення потужності сигналу до завади. Зловмисник апаратними засобами може продукувати шуми, а отже впливати на значення вказаного показника, що може спричинити некоректне визначення позиції та ідентифікації зловмисника.

Аналогічні наслідки можуть бути при реалізації зловмисниками в мережі релейної атаки. У цьому разі декілька зловмисників зв’язані між собою через мережу на великій відстані один від одного. Один зчитує дані з тегу особи-жертви, яка знаходиться далеко від приймача, а інший, розташований у зоні дії приймача, отримує сигнал через мережу від першого і транслює його радіоприймачу, маскуючись під жертву.

Бездротова технологія зв’язку UWB характеризується незначними витратами енергії, використовує як несучі надширокосмугові сигнали з невеликими значеннями спектральної щільності потужності. Пристрої UWB можуть вимірювати відстань та координати об’єкта з високою точністю, оскільки їх сигнал краще проходить крізь перешкоди, ніж сигнал існуючих бездротових мереж, таких як Wi-Fi та Bluetooth. Характеристики найпопулярніших UWB чипів регулюються двома стандартами: більш старим 802.15.4a та сучасним 802.15.4z.

Оцінка відстані між анкором та тегом за UWB технологією ґрунтується на використанні часу поширення сигналу, тому релейні атаки в цьому разі не спрацьовують. Крім того, стандарт 802.15.4z містить покращення, що забезпечує протидію, наприклад, таким поширеним фізичним атакам, як раннє виявлення та запізніла фіксація (ED/LC – Early-Detect and Late-Commit), цитада тощо [15].

Під час атаки ED/LC зловмисник завчасно дізнається про структуру сигналу передавача тега тривалістю T_{sym} та значення його символів (рис. 2, *а*) і приймає сигнал передавача із затримкою (рис. 2, *б*), щоб пізніше ввести в оману приймачі сигналу щодо часу його надходження.

На цьому етапі (етапі раннього виявлення) приймач зловмисника виділяє початкову частину сигналу (перший символ) в межах часового проміжку $T_{ED} < T_{sym}$ (рис. 2, *б*). Це можливо здійснити, оскільки зловмисник може розмістити свій приймач на незначній відстані до передавача.

У подальшому зловмисник формує сигнал за структурою, подібною до прийнятого сигналу від тега, але з послабленою початковою частиною на інтервалі T_{ED} та підсиленим залишком у межах T_{LC} так, щоб забезпечити більше значення відношення сигнал/завада для сформованого ним результуючого сигналу (рис. 2, *в*).

Сформований у такий спосіб сигнал зловмисника фіксується UWB чіпом на камері (анкором) з випередженням на часовий проміжок T_a за дійсний від тега. Ця обставина є критичною з огляду на те, що впливає на точність розрахунку відстані до тегів, а отже, і співробітників у приміщенні. Так, за значення $T_a = 200$ нс похибка може становити близько 60 м.

Є низка методів визначення координат місцезнаходження пристрою, тобто розв'язання задачі позиціонування об'єкта в просторі на основі UWB технології, зокрема метод різниці прибуття (TDoA - Time Difference of Arrival) та метод двостороннього діапазону (TWR - Two Way Ranging).

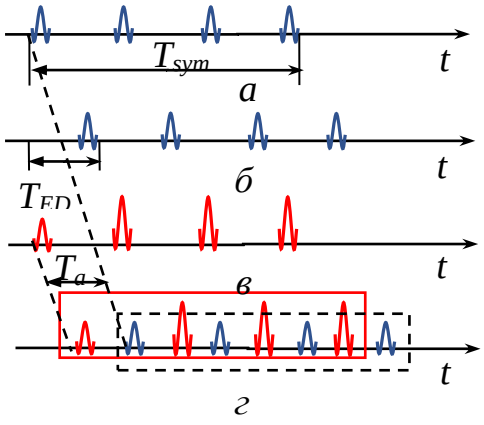

Рис. 2. До принципу дії ED/LC атаки
Джерело: розроблено авторами.

Метод різниці прибуття TDoA ґрунтується на тому, що тег особи розсилає так звані блінк повідомлення. Інші теги сприймають це повідомлення, але не реагують на нього. Блінк повідомлення досягає кожного з анкорів за різні проміжки часу, а отже в різні моменти часу, оскільки вони розміщені на різній відстані від тега особи. Різниця в часі між надходженням блінк повідомлень до анкорів і є основою для розрахунку просторових координат тега, а отже, і особи.

Однією з істотних негативних особливостей класичної реалізації методу TDoA є необхідність синхронізації функціонування анкорів, оскільки встановлено, що неточність синхронізації у 3 нс спричинює похибку близько 1 метра. Застосування додаткового спеціального обладнання дає змогу вирішити проблему синхронізації в системах позиціонування в режимі виміру реального часу на основі методу TDoA. Однак, таке рішення призводить до збільшення витрат на 20-40 %.

До переваг систем позиціонування на основі методу TDoA відносять достатньо великий термін використання батареї тегів, можливість зміни кількості як анкорів, так і тегів залежно від частоти надсилання тегами блінк повідомлень.

Метод двостороннього діапазону TWR регламентується стандартами ISO/IEC 24730-5 та IEEE 802.15.4-2011 і дає змогу визначити час поширення сигналу UWB, а потім розрахувати відстань між вузлами шляхом множення часу на швидкість світла. Така процедура з урахуванням особливостей TWR реалізується для одного тегу і всіх використовуваних в системі анкорів поступово у відповідний проміжок часу.

Для визначення відстані від тега до анкора необхідно обмінятися трьома повідомленнями: повідомленням-запитом, повідомленням-відповіддю та результуючим (фінальним) повідомленням (див. рис. 3). Тег ініціалізує TWR, надсилаючи повідомлення-опитування на відому адресу анкора у визначений час $T_{НЗ}$ (час надсилання опитування). Анкор фіксує момент прийому повідомлення-опитування $T_{ПЗ}$ і відповідає на повідомлення в момент часу $T_{ПВ}$. Тег при отриманні повідомлення-відповіді фіксує момент часу його надходження $T_{ВВ}$, формує фінальне повідомлення та надсилає його анкору в момент часу $T_{ФВ}$. Фінальне повідомлення містить його ідентифікатор, а також значення моментів часу $T_{НЗ}$, $T_{ВВ}$ та $T_{ФВ}$.

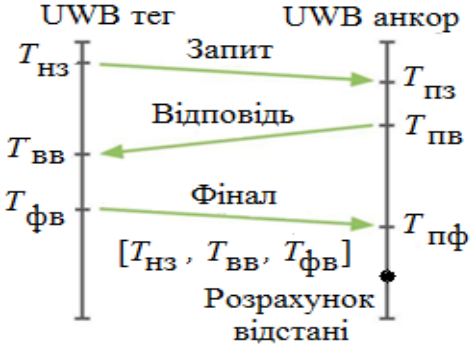

Рис. 3. До визначення відстані між тегом та анкором за TWR методом

Джерело: розроблено авторами.

З урахуванням моменту часу прийому фінального повідомлення $T_{ПФ}$ та даних, що в ньому містяться, анкор обраховує час поширення сигналу UWB та відстань між тегом та анкором. За бажанням, отримане значення відстані можна надіслати в зворотному напрямку до тега в повідомленні-звіті або до сусіднього анкора. Установлено, що оптимальна відстань між тегом і анкором для методу TWR становить 20…30 м.

Отже, для обчислення відстані до одного тега, потрібно запустити процес TWR з усіма анкорами в системі. Очевидно, що чим більше анкорів, тим більше часу потрібно для завершення всіх процедур TWR для одного тега.

Системи позиціонування, У яких реалізовано метод TWR, не потребують синхронізації пристроїв UWB. І це є їх істотною перевагою. Однак для таких систем число робочих тегів і термін служби джерел їх живлення здебільшого залежить від необхідної частоти оновлення та кількості анкорів. Крім того, теги повинні знати адреси анкорів.

Зіставивши методи TDoA та TWR, для реалізації в системі обираємо останній через простоту реалізації і більшу точність з меншими ресурсними витратами.

Алгоритм роботи системи.

При старті системи теги знаходяться у блінк режимі, генеруючи через кожні 2-3 секунди повідомлення на анкори. Це дає змогу зменшити споживання електроенергії і не виконувати постійно TWR.

Камера, у свою чергу, на основі зображення визначає кількість людей у приміщенні та звіряє ці дані з даними за кількістю тегів, отриманих UWB анкорами. Якщо зазначені дані не співпадають протягом чотирьох ітерацій, система переходить у активний режим. У цьому режимі: 1) запускається TWR процес визначення відстані між анкорами та тегами; 2) на основі зображення камерами вимірюється відстань до людей у приміщенні; 3) будується так звана оптична карта з координатами всіх людей, присутніх у приміщенні, а також UWB карта розміщення у цьому ж приміщенні осіб із UWB тегами; 4) координати точок UWB карти, як еталону, порівнюються з координатами точок (людей) оптичної карти для виявлення наявності зловмисників.

Координати точок (L_x, L_y) на оптичній та UWB картах обчислюються за такими співвідношеннями:

$$L_x = [2\sqrt{p_1(p_1 - B)(p_1 - D2)(p_1 - D1)} / B];\ p_1 = (A + D2 + D1)/2;$$

$$L_y = [2\sqrt{p_2(p_2 - A)(p_2 - D3)(p_2 - D1)} / A];\ p_2 = (A + D3 + D1)/2,$$

де $D1$, $D2$, $D3$ – відстані між відповідними об’єктами; A, B – відстані між двома камерами чи анкорами; $p1$, $p2$ – потрібні для розрахунку координат параметри (див. рис. 4).

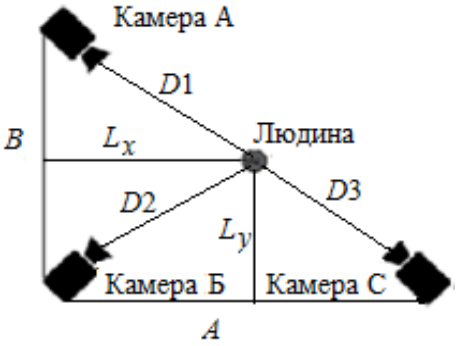

Рис. 4. До розрахунку координат
Джерело: розроблено авторами.

На етапі порівняння почергово для кожної UWB точки визначається кількість точок оптичної карти, які знаходяться в радіусі 0.5 метрів від UWB точки. Наявність однієї точки засвідчує про відповідність її координат одному зі співробітників, що знаходиться в приміщенні, а отже, його ідентифікацію на зображенні. Якщо в зазначену зону UWB точки потрапляє більше однієї точки оптичної карти, то це буде свідчити про присутність у приміщенні зловмисника. У подальшому система забезпечує його ідентифікацію та створює відповідні матеріали для відділу безпеки.

Висновки. В умовах жорсткої конкуренції необхідність протидіяти витоку інформації висуває додаткові вимоги до систем забезпечення контрольованого доступу до обладнання та приміщень об'єктів різноманітного призначення. На сьогодні при побудові таких систем дедалі частіше застосовуються бездротові технології та методи комп'ютерного зору. Розроблена та описана в роботі система виявлення проникнень ґрунтується на бездротовій UWB технології, дає змогу без розпізнавання облич ефективно та надійно ідентифікувати працівників установ та організацій і виявляти сторонніх осіб у режимі реального часу. При виборі для реалізації в системі бездротової технології автори виходили з того, що UWB технологія характеризується незначними витратами енергії, використовує як несучі надширокосмугові сигнали з невеликими значеннями спектральної щільності потужності, забезпечує достатньо високу точність визначення відстані до об'єкта та його координат.

Список використаних джерел

1. Identification and recognition. Required resolution [Electronic resource]. – Accessed mode: https://www.axis.com/learning/web-articles/identification-and-recognition/resolution.
2. Chanthaphone S. Design and implementation of security system for smart home based on IoT technology [Electronic resource] / S. Chanthaphone, Y. Lasheng. – Accessed mode: https://e-tarjome.com/storage/panel/fileuploads/2022-01-02/1641123351_E15914.pdf.
3. Suranthaa N. Design of Smart Home Security System using Object Recognition and PIR Sensor [Electronic resource] / N. Suranthaa, W. R. Wicaksonob. – Accessed mode: https://doi.org/10.1016/j.procs.2018.08.198.
4. Lens calculator/Axis Communications [Electronic resource]. – Accessed mode: https://www.axis.com/tools/lens-calculator.
5. Felzenszwalb P. A discriminatively trained, multiscale, deformable part model [Electronic resource] / P. Felzenszwalb, D. McAllester, D. Ramanan. – Accessed mode: https://cs.brown.edu/people/pfelzens/papers/latent.pdf.
6. Rich feature hierarchies for accurate object detection and semantic segmentation [Electronic resource] / R. Girshick, J. Donahue, T. Darrell, J. Malik. – Accessed mode: https://openaccess.thecvf.com/content_cvpr_2014/papers/Vemulapalli_Human_Action_Recognition_2014_CVPR_paper.pdf.
7. Girshick R. Fast R-CNN [Electronic resource] / R. Girshick. – Accessed mode: https://www.cv-foundation.org/openaccess/content_iccv_2015/papers/Girshick_Fast_R-CNN_ICCV_2015_paper.pdf.
8. Faster R-CNN: Towards real-time object detection with region proposal networks [Electronic resource] / S. Ren, K. He, R. Girshick, J. Sun. – Режим доступу: https://arxiv.org/pdf/1506.01497.pdf.
9. You only look once: Unified, real-time object detection [Electronic resource] / J. Redmon, S. Divvala, R. Girshick, A. Farhadi. – Accessed mode: https://www.cv-foundation.org/openaccess/content_cvpr_2016/papers/Redmon_You_Only_Look_CVPR_2016_paper.pdf.
10.SSD: Single Shot MultiBox Detector [Electronic resource] / W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.-Y. Fu1, A. C. Berg. – Accessed mode: https://arxiv.org/pdf/1512.02325.pdf.
11.Tan, M. EfficientNet: rethinking model scaling for convolutional neural networks [Electronic resource] / M. Tan, Q. V.Le. – Режим доступу: https://arxiv.org/pdf/1905.11946.pdf.

12.Murawski K. Method of Measuring the Distance to an Object Based on One Shot Obtained from a Motionless Camera with a Fixed-Focus Lens [Electronic resource] / K. Murawski. – Accessed mode: http://przyrbwn.icm.edu.pl/ APP/PDF/127/a127z6p04.pdf.

13.Lin Y. An Improved Sum of Squared Difference Algorithm for Automated Distance Measurement [Electronic resource] / Y. Lin, Y. Gao, Y. Wang. – Accessed mode: https://www.readcube.com/articles/10.3389/fphy.2021.737336.

14. An Indoor Ultrasonic Positioning System Based on TOA for Internet of Things [Electronic resource]. – Accessed mode: https://www.researchgate.net/publication/311165132_An_Indoor_Ultrasonic_ Positioning_System_Based_on_TOA_for_Internet_of_Things/link/618508afa767a03c14f7c15c/download.

15.Singh M. UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks [Electronic resource] / M. Singh, P. Leu, S. Capkun. – Accessed mode: https://eprint.iacr.org/ 2017/1240.pdf.

References

1. Identification and recognition. Required resolution. https://www.axis.com/learning/web-articles/identification-and-recognition/resolution.

2. Chanthaphone Sisavatha, Lasheng Yub. Design and implementation of security system for smart home based on IoT technology. https://e-tarjome.com/storage/panel/fileuploads/2022-01-02/1641123351_E15914.pdf.

3. Nico, Suranthaa, Wingky, R. Wicaksonob (2018). Design of Smart Home Security System using Object Recognition and PIR Sensor. https://doi.org/10.1016/j.procs.2018.08.198.

4. Lens calculator/Axis Communications. https://www.axis.com/tools/lens-calculator.

5. Felzenszwalb, P., McAllester, D., & Ramanan, D. (2008). A discriminatively trained, multiscale, deformable part model. http://people.cs.uchicago.edu/~pff/papers/latent.pdf.

6. Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2014). Rich feature hierarchies for accurate object detection and semantic segmentation. https://www.cv-foundation.org/openaccess/ content_cvpr_2014/papers/Girshick_Rich_Feature_Hierarchies_2014_CVPR_paper.pdf.

7. Girshick, R. Fast R-CNN. https://www.cv-foundation.org/openaccess/content_iccv_2015/ papers/Girshick_Fast_R-CNN_ICCV_2015_paper.pdf.

8. Ren, S., He, K., Girshick, R., & Sun, J. (2016, January). Faster R-CNN: Towards real-time object detection with region proposal networks. https://arxiv.org/pdf/1506.01497.pdf.

9. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. https://www.cv-foundation.org/openaccess/content_cvpr_2016/papers/ Redmon_You_Only_Look_CVPR_2016_paper.pdf.

10. Liu , W. et al. (2016, December). SSD: Single Shot MultiBox Detector. https://arxiv.org/pdf/1512.02325.pdf.

11.Tan, M., Le, Q.V. (2020, September). EfficientNet: rethinking model scaling for convolutional neural networks. https://arxiv.org/pdf/1905.11946.pdf.

12.Murawski, K. (2015, Cherven). Method of Measuring the Distance to an Object Based on One Shot Obtained from a Motionless Camera with a Fixed-Focus Lens. http://przyrbwn.icm.edu.pl/ APP/PDF/127/a127z6p04.pdf.

13. Lin Y., Gao Y., & Wang, Y. (2021, August). An Improved Sum of Squared Difference Algorithm for Automated Distance Measurement. https://www.readcube.com/articles/10.3389/ fphy.2021.737336.

14.An Indoor Ultrasonic Positioning System Based on TOA for Internet of Things. https://www.researchgate.net/publication/311165132_An_Indoor_Ultrasonic_Positioning_System_Bas ed_on_TOA_for_Internet_of_Things/link/618508afa 767a03c14f7c15c/download.

15.Mridula Singh, Patrick Leu, Srdjan Capkun. (2017). UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks. https://eprint.iacr.org/2017/1240.pdf.

Отримано 06.02.2023

UDC 004.77.056(045)

Mykola Humen[1], Dmytro Kushchevskyi[2]

[1]PhD in Technical Science, Associate Professor, Deputy Dean Faculty of Air Navigation,
Electronics and Telecommunications Faculty
National Aviation University (Kyiv, Ukraine)
E-mail: mbgumen@ukr.net. **ORCID:** https://orcid.org/0000-0001-7935-6496

[2]Master
National Aviation University (Kyiv, Ukraine)
E-mail: dima.kushhevskij@gmail.com

PENETRATION DETECTION SYSTEM BASED ON UWB TECHNOLOGY

Effective controlled access to the premises of institutions and organizations of various purposes is an urgent need today. An equally important task is the detection of intruders who entered the premises. In the conditions of fierce competition, the solution of these tasks is a certain guarantee of reducing cases of unauthorized access to information and technical resources of institutions and organizations.

The analysis of research and publications showed that little attention has been paid to issues of reasonable selection and design of employees identification systems and detection of intruders using wireless technologies and computer vision algorithms.

The purpose of the article is to develop a system for automatic identification of persons in a premises without faces recognition based on UWB wireless technology and computer vision algorithms.

Based on a comprehensive analysis of approaches to the design of personnel access control systems, advantages and disadvantages of methods and algorithms for selecting objects on the image, technologies for detecting people in premises, algorithms for calculating spatial coordinates of objects and measuring the distance between them, features of positioning systems and wireless standards communication RFID, BLE, WiFi, UWB, GPS, a system for detecting penetrations into premises of institutions and organizations based on UWB technology is proposed in the article.

The developed system makes it possible in real time to register the movement of persons, to respond to cases of illegal penetrations, reliably toidentify authorized employees, to detect unauthorized persons without faces recognition and complex machine learning algorithms, and generate appropriate materials for the security department. The basic components of the system are stereo cameras with built-in chips that support the UWB standard, UWB employee tags, a control server, a communication module with the server and the corresponding software.

Keywords: *access control system; penetration detection; attacker; anchor; tag; ultra-wideband technology; computer vision; convolutional neural network; wireless technology.*

Table: 4. Fig.: 4. References: 15.

Гумен М., Кущевський Д. Система виявлення проникнень на базі UWB-технології. *Технічні науки та технології.* 2023. № 1(31). С. 80-89.