Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань _____ *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність _____ *125 Кібербезпека*
(код і назва спеціальності)

освітній рівень _____ *магістр*
(назва освітнього рівня)

освітньо-наукова програма _____ *кібербезпека*
(код і назва кваліфікації)

На тему: *Підвищення ефективності систем контролю управління доступом за рахунок застосування новітніх біометричних показників*

Виконавець: студентка ІІ курсу, групи КБм-21

_____ **Кулеша Ганна Андріївна**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	Наконечний В. С.		
Рецензент	Сайко В. Г.		
Нормоконтроль	Фесенко А. О.		

Київ 2022

Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації

_____Н.В. Лукова-Чуйко

«_____» _____2022 року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студентці ***КБм-21*** (група) **Кулеші Ганні Андріївні** (прізвище ім'я по-батькові)

Тема дипломної роботи *Підвищення ефективності систем контролю управління доступом за рахунок застосування новітніх біометричних показників*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол №5 від 29.10.2021

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *процес захисту фізичного периметру безпеки.*

Предмет досліджень *новітні біометричні показники в системах контролю управління доступом.*

Мета *досягти підвищення ефективності систем контролю управління доступом за рахунок використання новітніх біометричних показників.*

Вихідні дані для проведення роботи *методи захисту фізичного периметру безпеки, системи контролю управління доступом.*

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *досягнення значущого підвищення ефективності а також зменшення кількості хибно-позитивних спрацювань в СКУД.*

Практична цінність *покращення ефективності контролю доступу до фізичних об'єктів для зацікавлених в підвищенні якості. використання СКУД організацій.*

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**	**Відмітка про виконання**
Уточнення постановки задачі	29.10.2022 – 15.11.2021	*виконано*
Розробка плану роботи	16.11.2022 – 11.12.2021	*виконано*
Аналіз основних технологій СКУД	12.12.2021 - 14.03.2022	*виконано*
Розгляд та аналіз використання біометрії в СКУД	15.03.2022 – 30.03.2022	*виконано*
Розгляд новітніх біометричних технологій	31.03.2022 – 10.04.2022	*виконано*
Ефективність новітніх біометричних технологій при двофакторній аутентифікації	11.04.2022 – 20.04.2022	*виконано*
Аналіз ефективності	21.04.2022 – 05.05.2022	*виконано*
Оформлення пояснювальної записки	05.05.2022 – 15.05.2022	*виконано*
Підготовка до захисту дипломної роботи	15.05.2022 – 20.05.2022	*виконано*

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *Зниження збитків через несанкціонований доступ.*

Соціальний ефект *Підвищення ефективності систем контролю управління доступом для організацій різного розміру та типу власності.*

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Наконечний В. С.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ Кулеша Г. А.
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

РЕФЕРАТ

Пояснювальна записка до дипломної роботи Підвищення ефективності систем контролю управління доступом за рахунок застосування новітніх біометричних показників» складається зі вступу, основної частини, що містить 4 розділи, висновків і списку використаних джерел та додатку.

Загальний обсяг роботи – 64 сторінки. Робота містить 4 рисунки, 2 таблиці. Список використаних джерел включає 45 джерел.

Об’єкт дослідження – процес захисту фізичного периметру безпеки.

Мета роботи – досягнення підвищення ефективності систем контролю управління доступом за рахунок використання новітніх біометричних показників.

Методи дослідження – методи аналізу наявних рішень та методи комбінаційного моделювання для досягнення поставлених цілей.

У роботі досліджено сучасні загрози фізичній безпеці та їх вирішення за рахунок використання новітніх біометричних технологій в системах контролю управління доступом (СКУД). Проведено аналіз наявних варіантів використання новітніх біометричних технологій в системах управління доступом. Запропоновано метод використання новітніх біометричних технологій як частини двофакторної аутентифікації для покращення показників ефективності СКУД.

Наукова новизна. Запропоновано метод забезпечення захисту фізичної безпеки від ймовірних спроб несанкціонованого доступу, за рахунок поєднання новітніх біометричних показників із звичним способом входу в двофакторній аутентифікації.

Актуальність теми. Першочерговою потребою кожної організації є забезпечення безпеки всієї наявної інформації та активів компанії, гарантії захисту їх цілісності, конфіденційності та доступності. Фізична безпека є надважливою та першочерговою потребою для забезпечення належного рівня захисту як фізичних об’єктів так і обмеженню доступу до усієї інформації та активів компанії. Системи контролю управління доступом безупинно покращуються та видозмінюються, але

все ще залишаються найважливішою складовою організації безпеки кожної організації чи підприємства.

Ключові слова: фізична безпека, системи контролю управління доступом, біометрія, інфрачервоний сканер, венозний малюнок долоні, двофакторна аутентифікація.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AI	–	Artificial Intelligence
FAR	–	False Acceptance Rate
FRR	–	False Rejection Rate
IoT	–	Internet-of-Things
IT	–	Information Technology
MFA	–	Multi Factor Authentication
PIN	–	Personal Identification Number
RTLS	–	Real-time locating systems
ПЗ	–	Програмне забезпечення
СКУД	–	Система Контролю Управління Доступом
ЦОД	–	Центр обробки даних

ЗМІСТ

ВСТУП

Актуальністю даної роботи є стійка потреба в сталому підвищенні рівня захищеності фізичних активів абсолютно кожної організації чи компанії різних форм власності. Попередження спроб несанкціонованого доступу є надважливим етапом організації безпеки, який при вмілій імплементації здатен вберегти як фізичні так і цифрові активи компанії. Унеможливлення потрапляння в офіс чи на територію підприємства потенційного зловмисника значно знижує ризики, які могли б виникати внаслідок застосування останніми наприклад соціальної інженерії, для втирання в довіру до потенційної жертви чи вивідування секретної інформації.

Основною задачею цієї кваліфікаційної роботи є аналіз новітніх біометричних технологій, які використовуються або можуть бути використані в СКУД, пошук та аналіз рішень, які можуть гарантувати значуще підвищення ефективності систем контролю доступу порівняно з усіма звичними рішеннями.

Науковою новизною цієї кваліфікаційної роботи є досягнення підвищення показників ефективності а також зменшення відсотку хибно-позитивних та хибно-негативних спрацювань в СКУД.

Системи контролю управління доступом є важливою складовою фізичного захисту інформаційної безпеки. Перед системами контролю управління доступом стоять не лише виклики у вигляді несанкціонованого доступу, але й потреба в зборі даних для моніторингу різноманітних показників.

Об’єктом дослідження є процес захисту фізичного периметру безпеки для збереження як інформаційних активів, так і матеріальних цінностей та активів. Попри значний перехід багатьох компаній на віддалений режим роботи, захист фізичного периметру безпеки залишається однією з найважливіших складових безпеки, яка має протистояти як вже давно відомим так і новим викликам потенційних загроз.

Предметом дослідження є новітні біометричні технології та використання таких показників в системах контролю управління доступом. На даний момент вони

вже є досить розвиненими, та починають набувати певної популярності та широкого застосування.

Біометричні технології гарантують досить високу якість аутентифікації та попереджають деякі з загроз та викликів до фізичного периметру безпеки компанії.

Стрімкий розвиток інформаційних технологій (ІТ) та їх впровадження в усіх сферах діяльності значно удосконалює і прискорює багато процесів із забезпечення охорони фізичного периметру безпеки.

Зараз при вході до багатьох компаній можна не побачити колись звичного всім охоронця чи вахтера. Їх давно замінили автоматизовані рішення безпеки та турнікети, а менеджери з фізичної безпеки можуть контролювати безпеку всього об’єкта не виходячи із теплого кабінету.

Метою даної випускної кваліфікаційної роботи є підвищення ефективності систем контролю управління доступом за рахунок використання новітніх біометричних показників людини.

Першочерговою потребою кожної організації є забезпечення безпеки всієї наявної інформації та активів компанії, гарантії захисту їх цілісності, конфіденційності та доступності.

Очевидно, що фізична безпека є надважливою та першочерговою потребою для забезпечення належного рівня захисту як фізичних об’єктів так і обмеження доступу до усієї інформації та активів компанії.

Використання різноманітних біометричних технологій є важливим кроком в розвитку корпоративних систем фізичної безпеки. Підтвердження особи при використанні інформації про її біометричні ідентифікатори стає майже безпрограшним рішенням багатьох викликів, які на даний момент часу вже може собі дозволити майже кожна компанії. Очевидно, що такі рішення не будуть настільки ж дешевими як звичайні картки-пропуски, проте і ціна на них, зважаючи на значне поширення таких технологій, вже не вважається захмарною чи непідйомною.

Тож основною та найважливішою перевагою є саме однозначне встановлення відповідності між особою та її даними в системі, що може гарантувати досить

високий рівень безпеки. Зрозуміло, що так як на даний момент всі ці рішення активно розвиваються, стовідсоткової гарантії ніхто поки давати не береться. Проте, залишаючи також альтернативні способи входу чи впроваджуючи двофакторну аутентифікацію, ризики незаконного проникнення на територію, яка знаходиться під захистом, стрімко прямують до нуля.

Запропоноване рішення може бути корисним для компаній різного типу власності, навчальних закладів та установ, на яких передбачений контроль доступу до певних об’єктів або приміщень. Дане рішення дозволить відділам внутрішньої безпеки та власникам компаній стати більш впевненими в захищеності своїх активів, а також дасть змогу ще більше переключитись з рутинного моніторингу на цікавіші та корисніші задачі з організації безпеки на підприємстві.

РОЗДІЛ 1
ОПИС СИСТЕМ КОНТРОЛЮ УПРАВЛІННЯ ДОСТУПОМ

1.1 Огляд систем контролю управління доступом

Система контролю управління доступом – це така система, яка дозволяє контролювати доступ до областей і ресурсів на певному фізичному об’єкті або комп’ютерній інформаційній системі. Серед найпоширеніших та відомих всім прикладів можуть бути абсолютно повсякденні речі, які кожен зустрічає та використовує заледве не кожного дня. Замок на дверях, по суті, є формою контролю доступу. Ще одним звичним всім засобом контролю доступу є PIN-код на банківському терміналі або банкоматі. Контроль доступу зазвичай є повсякденним рішенням безпеки, хоча й інколи може зустрічатись в найнепередбачуваніших місцях або процесах, як в секретних кнопках пультів управлінь важливих установ, так і в звичайних дитячих іграх.

1. Мобільний контроль доступу

Дослідницька компанія IHS Markit повідомила, що мобільні облікові дані є найшвидшим продуктом контролю доступу, який зріс приблизно на 150% між 2017 і 2018 роками. Вона передбачає, що в 2023 році буде завантажено понад 120 мільйонів мобільних облікових даних [1].

Компанії швидко впроваджують контроль мобільного доступу. При цьому 44% офісних працівників відзначають, що пандемія зробила контроль доступу ще більш важливою проблемою. У 2019 році опитування HID підрахувало, що 54% підприємств оновили або перейдуть на мобільну систему контролю доступу протягом наступних 3 років.

З огляду на явну зростаючу потребу та зростання мобільного доступу, можна припустити, що більше половини прогнозованих підприємств перейдуть від застарілих систем у найближчі роки, якщо вони ще цього не зробили [2].

Використання облікових даних на основі мобільних пристроїв є органічною еволюцією індустрії фізичної безпеки та контролю доступу. Практично 93% всього населення США користується смартфоном, більшість з яких постійно тримають пристрій під рукою. Крім того, картки-ключі незручні, оскільки вони є другими в рейтингу речей, які найчастіше забувають. Оскільки більшість карт-ключів є незашифрованими безпосередніми RFID-картами, які можна легко клонувати, мобільні облікові дані також пропонують більш безпечне рішення.

2. Хмарний контроль доступу

Хмарний контроль доступу впроваджується в середніх і корпоративних компаніях. Фізична безпека була пізно пристосована для хмари, особливо в середніх і корпоративних компаніях. Однак на сьогоднішній день більшість систем компаній працюють на хмарних системах.

Будь-яка з відомих систем напевне вже працює в хмарі, просто це може бути неочевидним: обмін повідомленнями, електронна пошта, CRM для продажів, інструменти маркетингу, інструменти підвищення продуктивності, IT-інфраструктура, хостинг веб-сайтів та багато інших вже працюють з використанням хмарних сховищ та потужностей для розрахунків.

Переваги хмарного контролю доступу [3]:

- Система може масштабуватися відповідно до потреб організації
- Постійні оновлення безпеки, які можна запустити миттєво
- Нульовий час простою
- Управління першим мобільним доступом
- Сотнями будівель керують із центрального розташування
- Надання або скасування доступу в режимі реального часу та віддалено
- Постійне резервне копіювання даних
- Швидка еволюція продукту

Це також піднімає питання про те, яка модель збору, аналізу та зберігання даних контролю доступу буде переважати в майбутньому: хмарні обчислення (які при передачі третій стороні стають відомими як послуга контролю доступу) або обчислення всередині організації на власних ресурсах.

У хмарних обчисленнях дані збираються та аналізуються в центрі, що забезпечує переваги потужності та масштабованості. Він також пропонує зручність керованого обслуговування та автоматичне оновлення програмного забезпечення.

IHS Markit прогнозує стабільний попит на модель SaaS для контролю доступу, особливо серед нових користувачів, таких як малий та середній бізнес. Було б не дивно побачити більше рішень, які також мають тенденцію до збільшення попиту [1].

У периферійних обчисленнях дані збираються та аналізуються на самому пристрої – будь то камера, пристрій для зчитування карт, панель сигналізації тощо. Основною перевагою граничних обчислень є набагато швидший час обробки – критичне, наприклад, для вказівки автономному транспортному засобу, чи гальмувати – і придатність для віддалених застосувань.

Замість того, щоб конкурувати, хмарні та периферійні обчислення доповнюють один одного і, ймовірно, залишаться тут принаймні на середній термін для використання в технології контролю доступу. Хмарний контроль доступу пропонує зручність та економічну ефективність серед інших переваг, тоді як периферійні обчислення підходять для віддалених додатків і, як стверджує Axis Communications, заощаджують витрати на матеріали та робочу силу (без проводки) та спрощують майбутні зміни [4].

Сучасні глобальні операційні центри (GSOC) вимагають великих приміщень, наповнених десятками екранів, які передають потокове відео та канали контролю доступу з усіх точок доступу. Швидка еволюція мобільних телефонів, пристроїв, підключених до хмари, і програмного забезпечення для виявлення аномалій дозволить уникнути вартості та складності GSOC. Аномалії будуть передані менеджерам безпеки безпосередньо на їхні телефони. Комп’ютерний зір виявить активного стрільця з пістолетом і негайно сповістить служби безпеки прямо на їхні телефони в будь-якій точці земної кулі. Результатом буде підвищена безпека в режимі реального часу.

Завдяки вдосконаленню Artificial intelligence (AI) та машинного навчання підозрілу активність можна виявити миттєво. Якщо людина зазвичай працює між

9:00 і 17:00 у будні дні, активність в межах офісу об 22:00 миттєво згенерує сповіщення для команд безпеки. Охоронцям не обов'язково бути приклеєними до екрана комп'ютера, спостерігаючи за кожною подією доступу через усі двері. Натомість їх час можна звільнити для патрулювання та спостереження за простором навколо них. Їм можна автоматично сповіщати про події прямо на телефон й відповідати на них у режимі реального часу.

У сфері фізичної безпеки спостерігається значний зсув у бік управління доступом у хмарі, завдяки величезним перевагам, які надаються з точки зору операційних покращень, підвищеної безпеки та легкого керування доступом на кількох сайтах, щоб отримати переваги безмежної масштабованості.

Керування доступом до кількох сайтів раніше було серйозно неоптимальним. Наприклад, якщо співробітник відвідує іншу філію, це вимагатиме сповіщення за кілька днів наперед, щоб підготуватися до свого прибуття з точки зору безпеки та доступу. Такі ручні процеси, як ці, крім незручності, призводять до більшого витоку облікових даних і невідповідності безпеки.

Впровадження хмарних систем стало новою тенденцією завдяки можливості керувати кількома сайтами в рамках однієї системи. Рівнями доступу можна легко керувати на всіх сайтах. Крім того, можна керувати глобальною інфраструктурою без шкоди для безпеки чи зручності. Насправді в цьому середовищі підвищується безпека, а зручність вища.

Covid-19 допоміг змінити парадигму контролю доступу до парадигми контролю присутності; тобто, наскільки важливо знати, хто входить у приміщення вашої організації, так само важливо знати, де знаходиться персонал у цих приміщеннях, забезпечити фізичну дистанцію, зменшити щільність місць загального користування, бути готовим до безпечної евакуації тощо.

Служби локації в реальному часі (RTLS) дозволяють організаціям відстежувати місцезнаходження всіх людей на об'єкті. RTLS також оптимізує використання простору, забезпечує кращу обізнаність про розташування активів і дозволяє ефективніше використовувати освітлення, HVAC та інші ресурси [5].

RFID, Wi-Fi і Bluetooth, інфрачервоний і стільниковий зв’язок є одними з кількох технологій, які використовуються для відстеження осіб, а також активів. Відомо, що уряд Гонконгу використовує цю технологію за допомогою браслетів, щоб геозонувати людей, які дали позитивний результат на COVID-19, і гарантувати, що вони не порушують карантин.

RightCrowd — один із постачальників, який має активні програми в цій галузі, в тому числі в середовищі відкритого офісу та в зонах високої безпеки науково-дослідного центру. RightCrowd використовує технологію Bluetooth як свою віртуальну основу.

Останній звіт Market Trends аналізує тенденції та драйвери ринку RTLS, прогнозує зростання до 2029 року та порівнює рішення таких компаній, як Zebra Technologies, Impinj, CenTrak і Versus Technology. Прогнози інших компаній розбивають використання RTLS на різних ринках, включаючи спортивні події [6].

У статті Behind the Cloud [7], автором якої є голова та генеральний директор Salesforce, Марк Беніофф розповідає про свій шлях до створення нової галузі: CRM на основі підписки. Це відкрило двері до моделі на основі підписки для бізнесу на відміну від застарілих мережевих систем.

Застарілому програмному забезпеченню та мережам CRM потрібні роки для інтеграції, постійне обслуговування та оновлення вручну. Вони були розроблені з урахуванням специфікацій для кожного окремого підприємства, яке воно обслуговує, що згодом зробило систему негнучкою, незграбною, трудомісткою та неймовірно дорогою.

Пан Беніофф створив модель, яка виправила проблеми, які створили нову індустрію на основі контролю кінцевих користувачів і щомісячної підписки, щоб сприяти гнучкості та підзвітності. Отже, сьогодні ця модель використовується в більшості бізнесу.

Розквіт безконтактних систем контролю доступу

Звіт ABI Research бачить речі по-іншому у світлі пандемії коронавірусу; він прогнозує значне зниження доходу від поставок біометричних пристроїв внаслідок

переходу роботи в дистанційний формат. Але є два винятки: розпізнавання облич і зіставлення райдужної оболонки ока.

Як повідомляє securityinfonews.com: «розпізнавання обличчя та райдужної оболонки ока стало ключовими технологіями, які дозволяють здійснювати аутентифікацію, ідентифікацію та стеження за користувачами та громадянами, які носять захисні головні убори, маски або, з частково закритими обличчями. Ці елементи, які раніше були прокляттям алгоритмів розпізнавання обличчя, тепер інтегровані в цінні пропозиції розробників алгоритмів».

Інший аналіз, який враховує COVID-19, пропонує ще один сонячний прогноз щодо розпізнавання облич у системі контролю доступу. Розпізнавання облич за допомогою аналізу ринку Edge Computing Report – Global Forecast to 2025 – Кумулятивний вплив COVID-19 прогнозує CAGR на 20% з 2019 по 2025 рік на основі «конфіденційності, пропускної здатності та інших потенційних переваг виконання розпізнавання країв обличчя безпосередньо на пристрої» [8].

По всьому світу офіси, фабрики, роздрібні магазини, ресторани, стадіони, театри, музеї, бібліотеки, готелі, банки та майже всі типи об’єктів, де розміщуються працівники, стояли порожніми або майже порожніми місяцями. Компанії повинні будуть поступово та з обережністю впроваджувати повернення персоналу на робочі місця в офісах. Зокрема, зусилля будуть прикладеними також до зміни організації контролю доступу для забезпечення актуальних гарантій безпеки.

Контроль доступу може стати більш детальним, можливо, зі знятими або відкритими дверями з низьким рівнем безпеки, зміненими коридорами та зведеними до мінімуму бар’єрами, яких часто торкаються.

Але заходи безпеки не повинні означати відмову від безпеки. Рекомендованими є такі заходи, як зміна годин роботи в системах контролю доступу, щоб відображати поточну політику, а також перевірку прав доступу та застосування підходу з нульовою довірою до доступу, якщо це можливо. Для початкового входу в будівлю або окрему зону чи об’єкт пропонується обмежити точки доступу до будівлі – один вхід і один вихід, якщо це можливо. Крім того,

компанії можуть направляти відвідувачів за стійки вестибюлів з окремими шляхами «вхід» і «вихід».

У той час як компанії розглядають довгострокові рішення для своєї технології контролю доступу, вони вживають недорогих короткострокових заходів, коли бачать, як розвивається пандемія. Наприклад, замість того, щоб використовувати закриття офісів для встановлення безконтактних систем контролю доступу, підприємства, які все одно можуть зменшувати свою площу, оскільки повернення до роботи залишається під сумнівом, розміщують дезінфікуючий засіб та/або серветки/паперові рушники по обидва боки дверей; тестування персональних брелків або пристроїв, схожих на гачки, за допомогою яких можна повертати дверні ручки, натискати кнопки ліфта та вмикати вимикачі світла; та розповсюдження масок й одноразових рукавичок.

Дані системи контролю доступу також можуть бути перевірені для відстеження контактів осіб, у яких позитивний тест на Covid-19. За даними securityworldmarket.com, «Часові рамки можна вказати до та після того, як людина, з позитивним тестом на COVID-19, увійшла на територію. Адміністратори також можуть отримувати файли звітів для експорту тих, хто потенційно заражений COVID-19, із можливістю приховувати імена позитивних чи виявлених осіб, щоб захистити особистість людей та обчислити ступінь зараження» [9].

Компанії з контролю доступу, постачальники відео та аналітичні компанії створюють системи для боротьби з коронавірусом, відстежуючи зайнятість робочих місць для забезпечення вимог фізичного дистанціювання. Різні компанії мають різні версії, кожна з яких базується на різних технологіях. І деякі компанії розглядають можливість віддалених центрів безпеки паралельно із повним збереженням функцій безпеки.

Та ж історія стосується технологій контролю доступу. Традиційно контроль доступу був бізнес-моделлю, керованою продажами обладнання. Ви купуєте зчитувачі, ключ-картки та панелі з розповсюдження, а інтегратор збирає та програмує локальний сервер. Оновлення потрібно програмувати вручну, а для роботи потрібен IT-персонал. Часи змінюються, як і наша культура та ландшафт

безпеки. Таким чином, ця модель зараз поступово припиняється і замінюється контролем доступу на основі підписки, який керується з хмари, щоб дати кінцевим користувачам необхідний контроль та гнучкість.

Тож, володіння контролем доступу має першорядне значення, коли люди прагнуть захистити важливу, конфіденційну інформацію та обладнання.

Контроль предметів або керування електронними ключами — це область всередині (і, можливо, інтегрована з) системи контролю доступу, яка стосується управління володінням і розташуванням невеликих активів або фізичних ключів. Фізичний доступ особі може бути дозволений залежно від оплати, авторизації тощо.

У фізичній безпеці термін контроль доступу відноситься до практики обмеження доступу до майна, будівлі чи приміщення уповноваженим особам. Фізичний контроль доступу може бути досягнутий людиною (охоронцем або секретарем), за допомогою механічних засобів, таких як замки та ключі, або за допомогою технологічних засобів, таких як системи контролю доступу, як-от приміщення. У цих середовищах управління фізичними ключами також може використовуватися як засіб подальшого керування та моніторингу доступу до областей із механічним ключем або доступу до певних невеликих активів.

Фізичний контроль доступу – це питання кому, де і коли. Система контролю доступу визначає, кому дозволено входити чи виходити, де їм дозволено виходити чи входити, а також коли їм дозволено входити чи виходити.

Історично це було частково здійснено за допомогою ключів і замків. Коли двері зачинені, тільки хтось із ключем може увійти через двері залежно від того, як налаштований замок. Механічні замки та ключі не дозволяють обмежувати ключницю певним часом або датою. Механічні замки та ключі не забезпечують записів ключа, який використовується на певних дверях, і ключі можна легко скопіювати або передати неуповноваженій особі. У разі втрати механічного ключа або утримувача ключа більше не має права використовувати захищену зону, замки необхідно повторно заблокувати.

Електронний контроль доступу використовує комп’ютери для вирішення обмежень механічних замків і ключів. На зміну механічним ключам приходить

широкий спектр облікових даних, серед яких є як електронні ключі, так і спеціальні біометричні показники, які виступають обліковими даними. Електронна система контролю доступу надає доступ на основі наданих облікових даних. Коли доступ надано, двері розблокуються на заздалегідь визначений час і транзакція записується. У разі відмови у доступі двері залишаються замкненими, а спроба доступу реєструється. Система також відстежуватиме двері та сигналізує, якщо двері примусово відкриті або утримуються відкритими занадто довго після відмикання.

В свою чергу СКУД зазвичай включає [10]:

• Пристрої, що перегороджують, виконавчі пристрої. Покликані виконати той чи інший «наказ» чи сценарій управління, під безпосереднім керівництвом вищих органів управління (контролерів чи розширювальних блоків). Наприклад, турнікети, двері обладнані керованими замками, ворота, шлагбауми, шлюзи тощо.

• Пристрої, що зчитують, «зчитувачі» (рідери). Пристрої введення, покликані повідомити органи управління деякі ідентифікаційні дані про об'єкт. Наприклад, пристрої радіочастотної ідентифікації (RFID), дактилоскопічні сканери, пристрої машинного зору тощо.

• Контролери СКУД, серце системи. Електронні мікропроцесорні модулі, що реалізують автентифікацію об'єктів доступу, логіку авторизації для доступу до тих чи інших приміщень та зон управління.

• Програмне забезпечення СКУД, необов'язковий елемент, що дозволяє здійснювати централізоване управління контролерами СКУД із персонального комп'ютера (ПК), формування звітів, може мати різноманітні додаткові функції, такі як облік робочого часу, тощо.

• Конвертори середовища для підключення апаратних модулів СКУД один до одного і до ПК. Також є необов'язковою складовою. Як приклад - деякі контролери СКУД вже мають інтегрований інтерфейс Ethernet, що дозволяє без використання будь-яких додаткових пристроїв підключатися до ПК, зв'язуватися один з одним. Також є контролери з інтегрованим Web-інтерфейсом, який дозволяє працювати з контролером безпосередньо через один з браузерів. Також є чимало автономних

контролерів, які не потребують та не мають можливості підключення до комп'ютерів або подібних контролерів.

• Допоміжне не інтелектуальне обладнання (блоки живлення, кнопки), з'єднувальні дроти.

1.2 Аналіз історичних аспектів систем контролю управління доступом

Для кращого розуміння поточної ситуації також важливо розуміти, якими були першопричини та потреби у виникненні контролю доступу як такого. Розвиток систем контролю управління доступом включає як старі, навіть древні технології, так і те, як вони еволюціонували до того стану, що ми звикли бачити сьогодні. Будь-який пристрій, який використовується для захисту чогось, можна визначити як замок, а все, що використовується для відкриття, можна назвати ключем.

Одні з перших механічних дерев’яних замків були виявлені в Ассирії (сучасний Ірак) ще в 4000 році до нашої ери, також одним із найдревніших систем контролю доступу може похвалитись гробниця фараона Тутанхамона, яка замкнена стародавнім мотузковим вузлом, як на рисунку 1.1 [11].

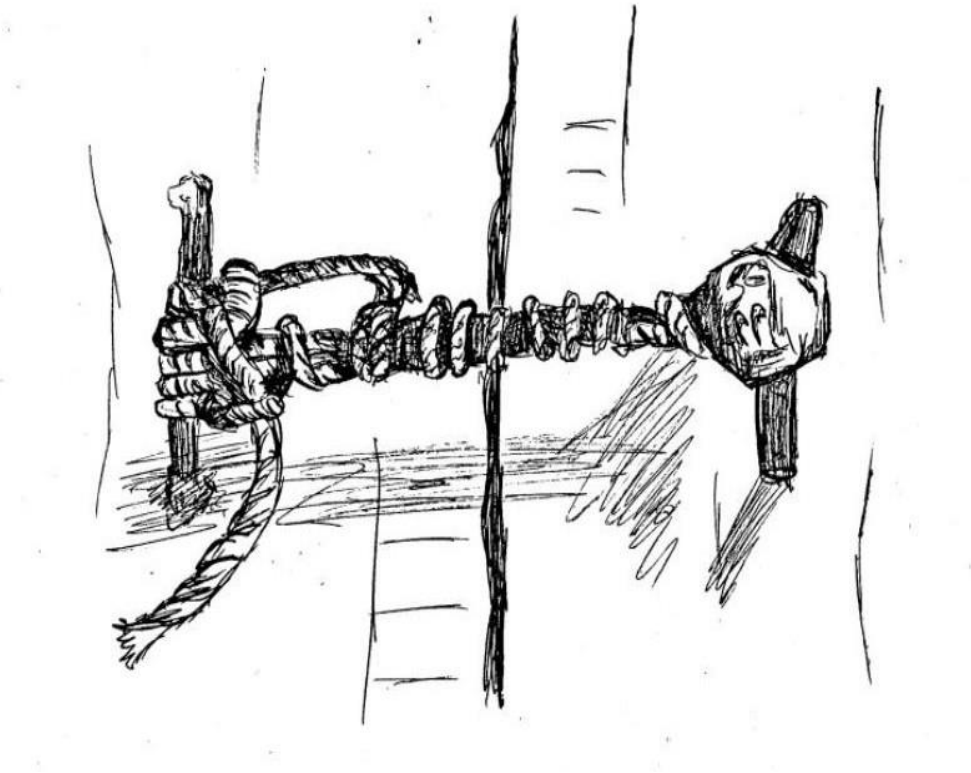

Рисунок 1.1 – Вигляд стародавнього мотузкового замка

Різні стилі захищеного замка з’являються протягом римського періоду, а також у стародавньому Китаї, принаймні, до часів раннього Шовкового шляху. Проте поширення замків могло відбутись набагато раніше і в ширших масштабах. Присутні історичні згадки, що через небезпеки в своєму суспільстві, римляни вважали, що потребують покращеної безпеки, порівняно з тією, яка була загальноприйнятою на той час.

Натхнені дерев’яними системами замків стародавніх греків, вони створили перші унікальні металеві ключі, деякі з них були достатньо малими, щоб використовувати їх одночасно і як ювелірні вироби, і як засоби, які могли б ефективно захищати майно та будівлі. Ця ідея і призвела до створення римського навісного замка, який згодом був удосконалений китайцями для використання на торгових шляхах, і в свою чергу надихнув на створення важких кованих замків, які використовувалися в Англії приблизно в 870-890 роках нашої ери [12].

Серед більш сучасних видів замків варто зазначити наступні [13]:

- важільний замок подвійної дії, який приписують Роберту Баррону в 1778 році;
- замки Джозефа Брама з’явилися в 1784 році;
- сучасна булавка подвійної дії була створена Лінусом в Єльському університеті у 1848 році, але вона базується на попередніх патентах і єгипетському шпильковому стакані.
- вафельні замки, які приписуються за патентом Філо Фелтеру, винайдено в 1868 році;
- дискові замки були винайдені Емілем Хенріксоном у 1907 році;
- замки Medeco з кутовою шпилькою йдуть у Roy Spain у 1960-х роках (дещо відмінні від тих, які зараз називають двоосьовими, але схожі за своїм принципом).

Проте контроль доступу — це значно більше, ніж просто замки, навіть з історичної ретроспективи. Щоб забезпечувати в ранні часи потрібну безпеку, у багатьох королівствах військові сторожі працювали в організовані зміни для

забезпечення цілодобового надійного захисту. Самим охоронцям було надано доступ лише в певні зони, у певний час, використовуючи складні процедури планування доступу та ідентифікації як ранню форму контролю доступу.

Певною мірою контроль доступу присутній навіть у старій архітектурі. Загальновідомо, що замки були побудовані з ровами навколо них і розвідними мостами як єдиною точкою входу, щоб уникнути вторгнення та нападу. Є також незліченна кількість прикладів використання сторожових веж для спостереження та охорони периметру та прилеглих територій. Як в стародавні, так і в більш сучасні часи, важливими були різноманітні інженерні рішення щодо контролю доступу та забезпечення захисту.

Міцні замки та споруди, що захищають від проникнення, існують з самого початку цивілізації. Але які ще приклади засобів забезпечення безпеки зустрічаємо в історії? Використання паролів переплітається з усією нашою історією як спосіб отримання доступу та перевірки. Це може включати використання пароля для входу до залів закладів, де алкогольні напої незаконно продавалися під час американської заборони, і використання кодових фраз для забезпечення безпеки військових місій і місць під час багатьох воєн. Незважаючи на те, що тепер це все еволюціонує до контактної інформації та біометричних даних, концепція паролів все ще залишається стандартом і основою для контролю доступу сьогодні.

Наприкінці 1800-х років, з винаходом лампочки та розширенням електрики, стало можливим мати працівників, які працювали навіть у найтемніші ночі. Оскільки ідея працювати вдень і вночі ставала все більш поширеною, зосередження на забезпеченні безпеки будівель і наданні доступу лише для відповідного робочого персоналу ставало все більш поширеним. Саме тоді використання годинників, детальних записів та журналів безпеки стало корпоративним обов’язком. І саме і ті часи безпека, управління персоналом та контроль робочого середовища почали розвиватися в те, що ми маємо станом на сьогодні.

Усі ці історичні елементи об’єдналися та розвинулися, щоб стати нашим щоденним контролем доступу. Загальний контроль доступу та всі його функції

мають глибоке коріння в історії, і це показує, наскільки надійним наріжним каменем контроль доступу є для нашої безпеки.

1.3 Роль СКУД в загальній структурі безпеки

Для розуміння цілісної картини також доцільним буде розглянути роль фізичної безпеки в загальній структурі безпеки, а також рівні, на які вона поділяється.

Фізична безпека — це комплекс заходів, яких можна вжити для захисту будівель, майна та активів від різного виду зловмисників [14]. Управління відвідувачами покликане бути першою лінією захисту будь-якої компанії чи організації. Система фізичної безпеки використовується для підвищення безпеки шляхом сканування ідентифікаторів та проведення перевірок даних аутентифікації для кожної особи, яка реєструється при вході, наприклад у вестибюлі чи на рецепції офісу компанії. Також важливою складовою системи фізичної безпеки є збір даних для різного виду моніторингів.

Розробка програми фізичної безпеки для компанії, закладу чи організації вимагає кількох наступних рівнів захисту [14]:

- зовнішнього периметра;
- внутрішнього периметра;
- внутрішньої частини будівлі.

Ефективна система фізичної безпеки зазвичай реалізує по дві або три форми безпеки на кожному рівні. Розглянемо детальніше кожен із рівнів захисту:

1. Безпека зовнішнього периметра.

Зовнішній периметр об'єкта визначається фактичними лініями власності, це може бути як паркан, так і зовсім непомітна для відвідувачів межа, яка є фактичною лінією власності, що підкріплено відповідними документами. При забезпеченні безпеки зовнішнього периметру, основна мета полягає в тому, щоб контролювати, хто може ходити або їздити на території, якщо її розміри це дозволяють. Охорона периметра може включати замкнені ворота, які можуть бути безпосередньо

зачинені, дистанційно керовані або захищені охороною. У деяких ситуаціях достатньо досить умовної межі, наприклад простий живопліт може забезпечити належну безпеку периметра установи з відносно вільною політикою відвідувань, тоді як огорожа з колючого дроту з охоронюваними воротами та спеціально навченими охоронцями потрібна в екстремальних або на локаціях із підвищеною небезпекою або потребою і додатковій безпеці в силу своєї специфіки. Для визначення, який тип захисту периметра доцільно встановити, потрібно зважити ризик доступу зловмисника до майна та порівняти його з вартістю доступних заходів фізичної безпеки.

Охорона периметра може включати природний контроль доступу та територіальне укріплення.

Природний контроль доступу використовує особливості будівлі та ландшафтного дизайну, щоб спрямовувати людей, які входять і виходять із території, на яку поширюється право власності. Теорія полягає в тому, що сприйняття ризику злочинцями знижується, якщо вони відчувають, що можуть пересуватися непомітно. Природні заходи контролю доступу можуть перешкодити цьому зниженому почуттю ризику та стримувати їх бажання наблизитися до майна чи будівлі. Природний контроль доступу повинен включати входи та виходи для ефективного запобігання зловмисникам та усунення будь-яких можливих шляхів евакуації.

Територіальне укріплення, посилення охорони відрізняє приватну власність від громадської власності або приміщень, щоб запобігти несанкціонованому проникненню. Це важливо для забезпечення уповноваженим особам відчуття панування. Уповноважені особи помітять відвідувачів, які здаються не на своєму місці, оскільки зловмисникам важко змішатися. Територіальне зміцнення має ту ж мету, що й безпека периметра: не допускати зловмисників на певну територію чи приватну власність.

2. Безпека внутрішнього периметра.

Охорона периметра захищає двері, вікна та стіни закладу. Системи сигналізації часто використовуються як попереджувальний сигнал при порушенні

входу або в’їзду; однак не кожна загроза, що проникає в будівлю, активує спрацювання тривоги. Заходи безпеки периметра включають замки, ключі, системи контролю управління доступом, електронні системи керування відвідувачами та ключі. Ці заходи допомагають не допускати сторонніх людей і контролювати потік відвідувачів у будівлю. Не кожна особа може розглядатись як загроза, яка проникає в будівлю, але використання таких технологій, як керування відвідувачами та управління доступами дозволяє створювати внутрішні списки спостереження, проводити планові та позапланові перевірки, забороняти вхід відвідувачам і негайно надсилати сповіщення охоронцям чи працівникам відділу безпеки, у випадку присутності загрози.

3. Внутрішня безпека.

Внутрішня безпека стосується внутрішніх приміщень будівлі, де знаходяться офіси співробітників, сховища даних та інші активи. Камери безпеки та детектори руху ефективні для моніторингу внутрішніх приміщень бізнесу. Електронні системи контролю доступу зупиняють несанкціонованих відвідувачів біля дверей та контролюють рух усередині закладу. Система керування відвідувачами, розташована у фойє, сканує ідентифікатори, записує час відвідування та зберігає ідентифікаційну інформацію про кожну людину, яка запитує доступ до відповідного закладу. VMS може запустити миттєву перевірку відвідувачів і попередити персонал про відвідувачів, які можуть становити загрозу, якщо їм буде дозволено вхід.

Однаково важливими є підвищення безпеки на кожному з рівнів. Планування системи безпеки з точки зору згаданих вище трьох рівнів може використовуватись частково, наприклад можна спробувати застосувати два або три заходи фізичної безпеки на кожному рівні для досягнення найкращих результатів. Найкраще залишатися проактивним, коли справа стосується управління ризиками та забезпечення безпеки співробітників і об’єктів.

Управління відвідувачами — є важливою частиною для завершення остаточного плану фізичної безпеки.

Система контролю доступу у сфері фізичної безпеки зазвичай розглядається як другий рівень безпеки фізичної структури.

Висновки за розділом 1

Інноваційні технології та методи в області управління ідентифікацією дозволяють змінити світ традиційної безпеки та полегшують перехід від фізичних облікових даних (проксі-карти контролю доступу та смарт-карти) до цифрових, електронних.

Загрози, на відміну від будь-яких раніше уявних, стали реальними та буденними; від клонованих облікових даних до компромісу базових комунікацій між традиційними компонентами безпеки. Щоб протистояти цим загрозам, потрібна здатність захищати та підтверджувати свою особу для авторизації прав доступу, безпечно та швидко передавати цю особистість, забезпечуючи при цьому конфіденційність та довіру.

Новатори створюють нові можливості для бізнесу разом із новими технічними та етичними проблемами, зміцнюючи традиційні способи безпеки. Системні архітектори вимагають ще більших знань про інформаційні системи, крім основи фізичної безпеки, щоб розгорнути надійні програмні та апаратні компоненти.

Менеджери з безпеки прагнуть покращити безпеку та підвищити зручність. Вони шукають способи підвищити задоволеність співробітників, перетворюючи процес вступу в безперешкодний досвід, водночас стверджуючи більш надійну аутентифікацію, яка запобігає зловживанню ідентичністю. Оскільки правила стають суворішими для центрів обробки даних, банківських сховищ та інших областей підвищеної безпеки, біометричні дані стають обов’язковими для сценаріїв дво- та трифакторної аутентифікації. З огляду на низькі витрати та ризик дублювання, традиційна картка та PIN-код не відповідають вимогам безпеки, які потрібні для впевненого захисту.

РОЗДІЛ 2
БІОМЕТРИЧНІ ТЕХНОЛОГІЇ В СКУД

2.1 Аналіз біометричних технологій в СКУД

Біометрія — це наука про унікальну ідентифікацію або перевірку особи серед певної групи людей шляхом вивчення фізіологічних або поведінкових характеристик користувача. Біометрична система безпеки нерозривно пов’язана з людиною, і тому її не легко зламати через крадіжку, змову або втрату, що робить її більш вигідною, ніж звичайні або традиційні методи аутентифікації, такі як особисті ідентифікатори та паролі, ключі чи магнітні картки [15].

Біометричні методи, такі як махання руками, сканування райдужної оболонки і зчитувачі для розпізнавання обличчя, готові до більш широкого застосування. Біометричні рішення для контролю доступу є швидкими, точними та безпроблемними. Для інтеграторів важливо зрозуміти потреби своїх клієнтів і усвідомити існування цих рішень та їх переваги.

Тож біометрія — це використання власних унікальних фізичних або поведінкових характеристик для ідентифікації та аутентифікації. Куди ви йдете, ваша біометрична інформація йде разом з вами. Біометрична технологія включає пристрій захоплення, будь то камера, оптичний датчик (контактний або безконтактний), клавіатура або мікрофон для отримання необроблених фізичних характеристик (необроблених даних). Ці дані потім перетворюються на довідковий шаблон, цифрове представлення з використанням, як правило, запатентованих математичних алгоритмів.

Біометричні характеристики включають обличчя, райдужну оболонку ока, долоню, відбитки пальців, вени пальців, голос, ходу та натискання клавіш. На відміну від паролів, біометричні дані є єдиним методом, який встановлює остаточний зв’язок між нашою фізичною та цифровою ідентифікацією. Біометричний ідентифікатор, шаблон посилання, може бути рядком чисел або

випадковим числом. Біометрія перевіряє та ідентифікує особу для системи контролю доступу, щоб визначити права або привілеї (доступ, послуги тощо), надані цій особі.

Метою біометричної аутентифікації є автоматизована перевірка особистості живої людини шляхом підтвердження якоїсь унікальної ознаки, якою володіє лише вона. Один тип біометричної аутентифікації орієнтований на фізіологію, наприклад, відбиток пальця, сітківку, райдужну оболонку ока, геометрію обличчя, вуха, руки або пальця тощо. Це зазвичай називають «статичною модальністю», оскільки імовірно ці біологічні властивості змінюються дуже мало або зовсім не змінюються. через деякий час. Крім того, біометричні ознаки ґрунтуються на нерухомих поверхнях тіла, будь то зображення долоні руки або малюнок судинних вен на руці.

Пандемія посилила деякі вже існуючі проблеми на ринку контролю доступу і змусила компанії впроваджувати нові технології швидше, ніж вони могли б зробити без появи вірусу. Наприклад, організації давно хотіли знати, хто і коли сторонні відвідувачі заходили та виходили з їхніх об’єктів з метою безпеки, але в умовах пандемії стає все важливішим знати, з ким кожен спілкувався у разі спалаху COVID-19.

Зміни способу життя та більшості звичних нам речей через пандемію COVID-19 змінили підхід до фізичної безпеки як у 2020-2022 роках, так і змінюватимуть надалі. З огляду на галузевий досвід, дослідження та прогнози, було виділено 5 основних тенденцій в системах контролю доступу на наступні декілька років [16]:

- мобільний контроль доступу, з використанням персональних пристроїв особи, що авторизується;
- хмарна безпека;
- багатофакторна аутентифікація;
- біометричні технології;
- бізнес-модель на основі підписки.

Побудова стійкого об’єкту та стратегії безпеки, яка протистоїть новітнім викликам, ще ніколи не була такою важливою, як зараз. Загалом, 5 основних тенденцій контролю доступу перетворюються на такі тренди в її організації [17]:

- поширення безконтактного контролю доступу;
- поширення нових технологій в сфері контролю доступу;
- організація зон покриття та інтеграція контролю доступу(так званий зональний контроль доступу).

Останнє десятиліття було потужним місцем для інновацій у технологіях контролю доступу. Як правило, контроль доступу був повільною галуззю, але відбулося справді величезне зрушення через чіткий попит клієнтів і потребу в впевненості у безпеці, яка чітко переходить у покращення систем контролю доступу.

Опитування 2019 року серед 473 директорів з безпеки, менеджерів і консультантів, проведене журналом HID Global and Security Management, визначило основні проблеми контролю доступу на той момент [18]:

- Інтеграція із застарілими системами (45%).
- Використання переваг нових технологій (39%).
- Захист від зростаючих уразливостей (38%).
- Зручність користувача та пропускна здатність на входах (36%).

Безпека більше не передбачає просто фізичний доступ, тепер він повинен охоплювати цифровий доступ і авторизацію на виконання транзакцій і послуг за допомогою персональних пристроїв. Приклади включають використання біометричних даних, вбудованих у мобільні пристрої, такі як мобільні телефони та електронні носії, для надання в режимі реального часу запитів на авторизацію для завершення транзакцій, систем доступу або переміщення даних. Електронні об'єкти та мережі, до яких можна підключити та отримати доступ за допомогою персональної електроніки, включають [19]:

- бортова комп'ютерна система в транспортних засобах, таких як автомобілі та скутери;
- медичні вироби, як зовнішні, так і всередині тіла;

- фінансові рахунки, платіжні системи та системи охорони здоров’я;
- розважальні платформи, такі як відеоігри та телебачення;
- різноманітні тренажери;
- зчитувачі дверей контролю доступу з технологією Bluetooth.

У світі цифрової безпеки всі вони вважаються «пов’язаними об’єктами». Біометричні рішення відіграють важливу роль у новому світі «пов’язаних об’єктів», щоб забезпечити верифікацію та довіру (певність) особистості для безперешкодного, безпечного фізичного та цифрового доступу. Біометрія гарантує, що лише уповноважена особа може отримати доступ до своїх «пов’язаних об’єктів». Це забезпечує спокій, гарантуючи, що поганий актор не зможе взяти під контроль бортовий комп’ютер автомобіля, медичний пристрій коханої людини або отримати доступ до безпечної зони чи мережі на робочому місці.

Два рішення, які привернули увагу протягом останніх двох років, – це підрахунок людей та моніторинг заповнюваності. Хоча ці рішення існували до COVID-19, найчастіше для бізнес-аналітики, зараз вони затребувані, щоб допомогти зупинити поширення вірусу. Також все більше уваги і попиту набуває відстеження контактів.

Біометрія існувала на периферії технології контролю доступу протягом десятиліть, обмежена високою вартістю, проблемами точності, конфіденційністю та іншими проблемами. Але зі зниженням цін, підвищенням якості та проблемами конфіденційності не на першому місці, вона стала життєздатною технологією контролю доступу в епоху COVID-19. Один з прогнозистів прогнозує, що «безконтактна біометрична технологія підніме хвилю, створену пандемією COVID-19, до CAGR (сукупний річний темп зростання) у 17,4% з 2020 по 2030 рік, при цьому світовий ринок зросте в п’ять разів і досягне 70 мільярдів доларів.

Біометрія існує вже більше століття, але в зв’язку з підвищеною проблемою безпеки компанії шукають більш надійні методи захисту своїх будівель і активів. Це може бути у формі біометричних даних і бажання дізнатися більше про технології, такі як розпізнавання відбитків пальців та різні інші форми біометричної аутентифікації для контролю доступу до сайту.

В даний час використовується багато методів біометричних технологій, і, крім того, що вони пропонують підвищену безпеку, це також означає менші вимоги до ресурсів на місці. Однак, щоб знати, які методи найкраще підходять для певного бізнесу чи власності, важливо розуміти відмінності між різними доступними на даний момент варіантами.

Технологія розпізнавання відбитків пальців. Ідентифікація за відбитками пальців використовується правоохоронними органами вже понад 100 років. Технологія працює, фіксуючи унікальний візерунок і графічні виступи відбитків пальців людини. Це забезпечує певний рівень надійності для контролю доступу до сайту, оскільки можна бути набагато впевненішими в тому, хто перебуває на сайті в будь-який момент часу.

Геометрія руки. Вимірюючи ширину, довжину, площу поверхні та товщину руки, ця технологія використовується вже понад 40 років, і на її точність не впливають такі елементи, як бруд, чи навіть шрами.

Сканування райдужної оболонки і сітківки ока означає, що фізіологічні характеристики кожного ока можна порівняти з біометричними профілями, які зберігаються для підтвердження особи перед доступом до сайту.

Розпізнавання обличчя. Використовуючи профілі даних про тривимірну форму обличчя, судинні та теплові структури та аналіз текстури шкіри, можна ідентифікувати користувачів. Накладаючи на карту риси обличчя, можна контролювати такі характеристики, як розмір, форма або взаємне розташування щелеп, вилиць і очей. Потім ця інформація перетворюється на шаблон і порівнюється з профілями даних, що зберігаються у файлі, щоб знайти відповідність. Для цілей контролю доступу до сайту лише користувачам, чиї функції відповідають шаблону, буде надано доступ, а сповіщення безпеки можуть виникати, коли неавторизовані користувачі намагаються отримати доступ до певного об’єкта.

Завдяки численним досягненням у технологіях, за останні кілька років розпізнавання облич стало частиною домінуючої тенденції, згідно з якою розпізнавання обличчя стає майбутнім контролю доступу. Це вже спостерігається в

технології мобільних смартфонів, завдяки якій сотні мільйонів пристроїв захищені за допомогою цієї технології.

Технологія розпізнавання обличчя надає людям безпечну форму авторизації, яку не могли зробити попередні методи, такі як ключ-карти. Ця біометрична технологія означає, що користувачам потрібно лише показати своє обличчя сканеру, а їхні унікальні профілі нададуть усі необхідні докази того, що вони мають право на участь.

Минули часи, коли потрібно було запам’ятати пароль або брелок для входу в будівлю – тепер можна отримати доступ швидко, легко та безпечно, використовуючи власні унікальні біометричні дані.

Крім цього, біометричні технології мають багато інших переваг, зокрема і зручності. Користувачам не потрібно пам’ятати та носити з собою фізичні токени, щоб увійти в будівлі. Крім того, хмарні системи дозволяють віддалено керувати безперешкодними оновленнями – зазвичай через додаток на мобільному пристрої.

Контроль доступу до сайту через хмарні системи означає можливість оновлення в режимі реального часу, що полегшує з’ясування того, хто з користувачів отримував доступ до яких областей і коли.

Серед ключових висновків: розпізнавання облич займе найбільшу частку ринку, оскільки стане широко запровадженим як для перевірки особи, так і для контролю доступу; інші технології для розвитку включають райдужну оболонку ока, долоню, вени, голос і безконтактні відбитки пальців; і попит на безконтактні біометричні дані серед державних установ зросте через проблеми громадської безпеки.

Системи розпізнавання облич традиційно були дорогими і недоступними. Дороге встановлення вимагає значних витрат на інтеграцію, щоб працювати поверх застарілих систем. Процес реєстрації був громіздким і вимагав черги людей для реєстрації на окремих станціях. Завдяки прогресу та інноваціям у біометричному контролі доступу встановлення є економічно ефективним і може конкурувати з вартістю альтернативних систем ключ-карт. Миттєва самостійна реєстрація та проста інтеграція зробили розпізнавання обличчя доступнішим, ніж раніше. Хмарні

інформаційні панелі дозволяють адміністраторам централізувати керування доступом. Критичні вимоги до системи доступу з розпізнавання обличчя включають наступне [20]:

1) 2D і 3D розпізнавання обличчя;
2) постійне навчання з часом, щоб адаптуватися до змін обличчя;
3) запобігання спробам обдурити систему, використовуючи фото чи відео людини (анти спуфінг);
4) легка реєстрація;
5) робота з врахуванням різних демографічних показників;
6) суворий контроль конфіденційності та обмеження використання даних.

2.2 Аналіз переваг та недоліків використання біометричних технологій в СКУД

Чи покращує використання біометрії безпеку? Відповідь на це майже риторичне запитання є цілком логічною.

Переваги біометричної аутентифікації як способу підвищення рівня кібербезпеки присутні як на особистому так і на корпоративному рівнях. Але також важливо розуміти, чому саме біометричні технології покращують безпеку і які насправді переваги та недоліки присутні.

В першу чергу, можна зазначити відсутність паролів для крадіжки. На паролі припадає близько 81% випадків злому даних, що робить їх найбільшим недоліком особистої та корпоративної безпеки. Біометрія дозволяє компаніям замінювати паролі та токени простим у використанні, але безпечним рішенням, усуваючи загрозу, яку представляють паролі, і покращуючи загальний контроль доступу за допомогою підтвердження особи [21].

Основна перевага, яку біометрична аутентифікація забезпечує — це доказ того, хто стоїть за транзакцією. Незалежно від того, чи здійснюється це оплата чи вхід на віртуальний сервер чи в серверну кімнату, біометричні дані вимагають фізичного компонента, яким насправді є користувач. І тільки конкретний

користувач повинен бути фізично присутнім, щоб отримати доступ до потрібного об’єкта. Контроль доступу на основі ідентифікаційних даних є значним покращенням у порівнянні з альтернативними факторами аутентифікації – тим, що ви знаєте, або тим, ким ви є – оскільки їх можна позичити, продати або вкрасти. Тільки біометричні дані підтверджують особу, а не просто надають доступ.

Покращення конфіденційності теж є важливою перевагою використання біометричних даних. Хоча однією з найбільших проблем, які турбують споживачі щодо біометричних даних, є конфіденційність, правильно реалізоване рішення біометричної аутентифікації фактично покращує особисту конфіденційність. Коли біометричні дані зашифровані та безпечно зберігаються за допомогою таких методів, як візуальна криптографія та розподілена модель даних, це різко знижує ризик компрометації біометричних даних користувача в результаті порушення даних, не кажучи вже про зниження ризику самого порушення даних.

Це лише кілька переваг, які надає біометричний захист. Використання біометричних даних для багатофакторної аутентифікації замість комбінацій паролів і маркерів оптимізує зручність і безпеку для всіх учасників і допомагає компаніям підготувати свою інфраструктуру управління ідентифікацією та доступом до майбутніх розробок у сфері безпеки та конфіденційності. Проте, в кінцевому підсумку, доказом є досягнення багатьох компаній у своїх стратегіях безпеки, включаючи біометричну аутентифікацію.

Усі, від банків до виробників мобільних телефонів, запровадили біометричний захист. Від датчиків відбитків пальців до програмного забезпечення для розпізнавання обличчя, біометричні дані стають частиною повсякденного життя, і ми довіряємо їм більше, ніж паролям, що запам’ятовуються. Незважаючи на це, їх можна вкрасти або змінити, а датчиками можна маніпулювати.

Якщо кіберзлочинці успішно зламають біометричні дані, вони можуть легко отримати доступ до особистих даних, прихованих за відбитком пальця чи іншим біометричним ідентифікатором.

Біометрична технологія звучить як ідеальне рішення для слабких, спільних і повторно використовуваних паролів. Відбитки пальців та обличчя унікальні та не

можуть бути випадково залишеними чи загубленими. Крім того, кожен біометричний ідентифікатор такий же складний, як і будь-який інший, «простий» ідентифікатор не є актуальним в даному випадку. Вони здаються найпростішим і безпечним методом захисту та доступу до даних.

Однак вони також не можуть бути ідеальним варіантом без жодних додаткових умовностей. Якщо біометричні дані скомпрометовані в результаті витоку, їх не можна легко змінити, як наприклад паролі, і тоді біометричний ключ може бути отриманий з невеликими зусиллями кимось із наприклад близьких.

Але хіба біометричні дані не складніше зламати, ніж паролі?

За інформацією від компанії WatchGuard, перші вразливості були зафіксовані ще на початку двохтисячних [22]: «У 2002 році дослідник обдурив сканер відбитків пальців за допомогою клейких ведмедиків, а хакерська група аматорів перемогла TouchID iPhone у 2013 році. У 2017 році в'єтнамська група безпеки стверджувала, що створила маску, яка може обдурити FaceID Apple. Це лише питання часу, коли хакери вдосконалять ці методи та використають зростаючу тенденцію біометричних даних як єдиної форми аутентифікації».

Одним з прикладів біометричного злому є світ мобільних телефонів. У Samsung Galaxy S8 зламали сканер райдужної оболонки ока. У Samsung заявили, що для злому потрібна виключно малоймовірна ситуація, коли необхідне володіння райдужною оболонкою ока власника смартфона з високою роздільною здатністю, ІЧ-камерою, контактною лінзою та володінням смартфоном одночасно [23].

Дослідники продемонстрували, що розпізнавання голосу можна зламати, якщо злочинець має сто 5-секундних речень. Отримавши зразок, вони можуть подати зразок у комп'ютерну програму для відтворення мови. Китайські дослідники також продемонстрували здатність надсилати ультразвукові повідомлення до інструментів розпізнавання голосу, таких як Amazon Alexa [24].

Якщо роботодавці зберігають біометричні дані у великих базах даних, то спритні хакери будуть шукати вразливі сховища особистих даних, відбитків пальців і сканів сітківки ока.

Однією з тривожних тенденцій є те, що біометричні дані зараз використовуються як однофакторна аутентифікація, оскільки їм дуже довіряють. Але якщо кіберзлочинці успішно викрадають біометричні дані, вони можуть легко отримати доступ до особистої інформації, прихованої за відбитком пальця, без будь-яких інших перешкод.

Біометричний злом поки що не призвів до жодного великого публічного злому. Приклади надійшли від дослідників або людей у контрольованих і спеціалізованих ситуаціях. Однак той факт, що з'явилися приклади, підкреслює наявність вразливості.

Біометричний злом на даний момент не поширений. Вживання додаткових заходів обережності, щоб вимагати код доступу або двофакторну аутентифікацію в поєднанні з використанням біометричної перевірки може зробити процес аутентифікації більш безпечним.

2.3 Постановка задачі до вирішення, двофакторна аутентифікація

Ще одним старим-новим трендом стає багатофакторна аутентифікація. Вона вже є звичною для організації доступу та підтримання цифрової безпеки, проте у фізичній безпеці та системах контролю доступу ще майже не зустрічається.

Мобільні облікові дані також використовуються як для мультимодальної, так і для багатофакторної аутентифікації. Мультимодальна автентифікація може означати підтвердження особи/отримання доступу за допомогою принаймні двох окремих біометричних даних або надання доступу за допомогою будь-якого з різних облікових даних, наприклад, ключ-картки або PIN-коду. Багатофакторна автентифікація означає необхідність підтвердити особу/отримати доступ через на принаймні два методи або облікові дані (включаючи те, що ви знаєте, маєте чи є), наприклад, відбиток пальця та пароль.

Багатофакторна аутентифікація зараз широко використовується в цифровому доступі. Наприклад, коли співробітник входить в електронну пошту компанії або інший конфіденційний веб-сайт, компанії потрібен інший метод для підтвердження

особи за допомогою одноразового токена через SMS або інший додаток для аутентифікації.

Двофакторна аутентифікація була потрібна для фізичної безпеки для певних вертикалей, таких як нафтові, газові та електростанції, як частина відповідності NERC в комунальних галузях та іншій критично важливій інфраструктурі. Тепер він також стає доступним для інших корпоративних клієнтів, які хочуть отримати більш розширений рівень безпеки. З появою мультимодальних зчитувачів, які підтримують ключ-картку, мобільний телефон, pinpad і біометричні дані в одному, зростає доступність використання двофакторної аутентифікації для більш широких розгортань.

І багатофакторний, і мультимодальний підходи мають значні переваги. Багатофакторна автентифікація є більш безпечною, ніж однофакторна. Це також допомагає організаціям відчувати себе комфортніше за допомогою єдиного входу, а єдиний вхід є улюбленим у користувачів, оскільки він значно спрощує доступ до мережі. Крім того, регулювання може вимагати багатофакторної аутентифікації для обробки особистої ідентифікаційної інформації.

Багатофакторна аутентифікація часто використовується споживачами під час зміни паролів облікових записів або виконання онлайн-транзакцій; їм буде запропоновано ввести PIN-код, надісланий через SMS або електронну пошту, наприклад, для підтвердження особи. Вони називаються push-повідомленнями, і є улюбленими для дослідницької та аналітичної компанії Gartner. В свій час Gartner передбачав, що до кінця 2019 року 50% підприємств, які використовують мобільну аутентифікацію, скористаються її як основним методом перевірки.

Мультимодальна аутентифікація, яка вимагає двох окремих біометричних даних, є набагато безпечнішою, ніж одна біометрична, але дорожча й вимагає багато часу. Мультимодальна аутентифікація, яка вимагає вибору кількох облікових даних аутентифікації, менш безпечна, але набагато зручніша, наприклад, якщо ви забудете свою картку-ключ, ви зможете ввести PIN-код на клавіатурі.

Аутентифікація блокчейн

Тим часом технологія блокчейн з’являється як претендент на перемогу по незвичності аутентифікації. Випадки використання Blockchain з’явилися майже в кожній програмі безпеки, і контроль доступу та аутентифікація не є винятком. Дослідники вже встановили підтвердження концепції, тому цілком ймовірно, що деякі системи контролю доступу будуть засновані на технології розподіленої книги або блокчейн. Згідно з дослідженням, проведеним в Університеті Саскачевана, «використовуючи потенціал Hyperledger Fabric і Hyperledger Composer, було впроваджено захищений від несанкціонованого доступу додаток для контролю доступу на основі дозволеного блокчейна для керування дозволами доступу до фізичних місць».

Цікавим аспектом є те, що блокчейн можна використовувати як постачальник аутентифікації. Уявіть, що можна автентифікувати себе в державних службах, банках, аеропортах та інших службах лише за допомогою лише присутності особи та технології блокчейн. Використовуючи свою пару ключів, користувачі реєструють свою особу в блокчейні. Цей зареєстрований ідентифікатор є частиною інформації, яка містить хеші кількох пов’язаних із ідентифікаторами атрибутів. Наприклад, їх ім’я, реєстраційний номер управління, відбиток пальця або іншу біометричну інформацію. Після цього такий користувач може перейти до визнаної сторони, яка перевірить хеші, раніше зареєстровані в блокчейні, і дозволить стороні, яка розпізнає, «спонсорувати» цю інформацію як правду в блокчейні. Інші сторони, які довіряють конкретній стороні, що розпізнає, тепер можуть довіряти ідентифікатору в блокчейні та використовувати його як механізм аутентифікації або ідентифікації.

Розпізнавання обличчя використовується для безконтактного контролю доступу, замінюючи доступ за відбитками пальців. Багато компаній поспішають запровадити телефонний доступ у стилі Face ID в будівлі та об’єкти. Використання контролю доступу з розпізнаванням обличчя забезпечує сучасний безконтактний доступ.

Кібер- та фізична інтеграція мала й матиме глибокі наслідки для технології контролю доступу. Колись окремі системи контролю фізичного та кібер-доступу часто функціонують безперебійно. Та сама технологія розпізнавання облич, яка

відкриває двері офісного пакета, також інтегрується з камерою, яка дозволяє охоронцю підтвердити вашу особу, і з вашим ПК, щоб надати вам доступ до мережі. Очікується, що в майбутньому ця тенденція лише посилиться.

Насправді, 36% установок контролю доступу в навчальних закладах зараз включають відеосистеми або системи виявлення вторгнення. Інтегроване хмарне рішення для контролю доступу та керування відео дозволяє користувачам безперешкодно відстежувати активність доступу та пов’язувати події біля дверей за допомогою інтегрованого відео [25].

Надання доступу може бути набагато швидшим, оскільки передані дані ідентифікації допоможуть створювати облікові записи та негайно налаштовувати рівні доступу. Постійне вдосконалення інтеграцій може надати адміністраторам та менеджерам набагато більш детальний контроль під час початкового налаштування, активного керування та деактивації.

Окрім того, збільшення зв’язку дозволяє централізовано керувати джерелом авторитетних ідентифікаційних даних і легко їх передавати. У той же час системи та програми краще включатимуть дані ідентифікації для забезпечення дозволів даного користувача в межах цього ресурсу.

Висновки за розділом 2

Фізична безпека стає не тільки загальною проблемою об'єктів, але, більш фундаментально, проблемою ІТ. Захист активів компанії неможливий без урахування їх цінності в ІТ-інфраструктурі, за межами рівня безпеки мережі за допомогою брандмауерів та антивірусних програм. Запобігання доступу до фізичних машин і мереж за допомогою біометричних облікових даних відповідає ширшій індустріальній тенденції поступової відмови від таких легко скомпрометованих методів, як паролі та контакти.

Традиційні системи контролю доступу дозволяють фізичний доступ до приміщень на основі отримання розпізнаного номера картки та дозволяють логічний доступ до мережі або програми на основі отримання визнаного імені користувача та

пароля. Особа не ідентифікується, а розпізнаються картка, ім’я користувача та пароль. Додавання біометричної ідентифікації дає менеджерам з безпеки впевненість у тому, що особа фізично присутня і що облікові дані не можна передати чи клонувати.

Тож, технологія ідентифікації та аутентифікації, від програмного забезпечення до біометричного обладнання, продовжує розвиватися, про що свідчить зростаюче застосування низки державних і оборонних програм у відповідь на посилені загрози безпеці, міжнародні програми ідентифікації, а також розширення доступу до хмарного хостингу і системи ідентифікації, які встановлюються інтеграторами як для державних, так і для комерційних сайтів.

Найвідоміші тенденції безпеки 2021 року, на думку асоціації індустрії безпеки включають безконтактні рішення, які не потребують безпосереднього контакту особи із поверхнею сканера чи іншого пропускного пристрою, розпізнавання облич, хмарні обчислення та перехід до моделей обслуговування [26].

РОЗДІЛ 3
ЗАСТОСУВАННЯ НОВІТНІХ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ

3.1 Аналіз новітніх біометричних технологій

Замість того, щоб не забувати носити з собою картку-ключ, щоб зайти в офіс, співробітники можуть підтвердити свою особу за допомогою новітніх біометричних технологій.

Контроль доступу слідує сучасним технологічним тенденціям простоти та зручності, що на цьому ринку зазвичай означає використання безконтактної технології. Безконтактні рішення не потребують безпосереднього контакту особи зі сканером чи іншим пристроєм аутентифікації. Користувачам не потрібно турбуватися про те, що вони запам’ятовують свої фізичні дані або контактують з «високою точкою дотику» під час підвищеної турботи про гігієну.

Як і багато всього іншого у нашому світі, пандемія COVID-19 перевернула індустрію безпеки з ніг на голову. До пандемії використання відбитка пальця, щоб відімкнути двері, було трохи футуристичним. Але тепер ідея притиснути пальцем до загальнодоступного сенсорного екрану здається пережитком далекого минулого. І навпаки, сканер, який вимірює вашу температуру до того, як ви сядете в ліфт, колись міг здаватися зайвим втручанням в особистий простір, але тепер здається не лише безпечним, але й може демонструвати співробітникам та відвідувачам певної організації турботу про здоров’я і особисту безпеку.

Пандемія COVID-19 нерівномірно вплинула на біометричні технології. З одного боку вона була поганим чинником для форм біометричних даних, які вимагають контакту (наприклад, сканування відбитків пальців), але з іншого боку вона також викликала великий інтерес до безконтактної біометричної інформації та її застосування з метою як і підвищення рівня захищеності так і з метою збереження здоров’я.

З огляду на це, пандемія COVID-19 серйозно змінила ринок контролю доступу і багато в чому прискорила його еволюцію.

З новими досягненнями в галузі штучного інтелекту та біометричних технологій, у світі, що швидко змінюється, розвивається все більше і більше випадків використання біометричних технологій не зважаючи на тенденцію дистанційної роботи та віртуальної взаємодії між співробітниками та клієнтами під час та після дії карантинних обмежень спричинених пандемією COVID-19. Проте, всі виклики та необхідність захисту цінних бізнес-процесів, майна та активів компаній залишаються актуальними і на даний момент.

Перехід до віддаленої роботи також спричинив певну модифікацію вимог до захисту фізичних місць бізнесу, оскільки соціальне дистанціювання та правила ведення частково або повністю безконтактного бізнесу значно обмежують доступ до офісів як для частини співробітників, так і для клієнтів.

Окрім того, біометричні технології просунулися настільки, що починають замінювати традиційні методи безпеки. Наприклад, біометричний доступ є більш безпечним і надійним, ніж використання паролів чи вже звичним всім електронним карткам із чипом всередині та фотографією співробітника зверху. Оскільки біометричний маркер (наприклад, відбиток пальця, скан сітківки ока чи сканер венозного малюнку долоні) завжди доступний користувачеві і не може бути забутий (або вкрадений), він надає значні переваги над усіма іншими засобами автентифікації особи. Звісно, така значна та очевидна перевага заохочує підприємства використовувати біометричні технології для організації контролю та управління доступом на своїй території.

Усі ці варіанти використання біометричних даних покращуються в поєднанні з використанням штучного інтелекту. Програма штучного інтелекту здатна аналізувати неймовірні обсяги даних і використовувати цей аналіз для прийняття рішень. Це також може використовуватись, для надання програмам безпеки набагато глибшого розуміння правильності введених даних і зменшити хибнопозитивні або хибнонегативні спрацювання систем контролю управління доступом. Наприклад, такі інструменти, як розпізнавання обличчя та голосу, разом з

алгоритмами виявлення шахрайства та несанкціонованого доступу, можна навчати на біометричних даних, для значного підвищення їх ефективності.

Хоча штучний інтелект може здатися технологією, яка більше підходить для цифрової безпеки, очевидно, вона також може значно підвищити фізичну безпеку. У поєднанні з хмарними системами та біометричним контролем доступу, штучний інтелект може запропонувати багато переваг перед традиційними ключами, електронними картками та охороною. Такі програми можуть включати розпізнавання голосу, обличчя, чи інших біометричних показників для ідентифікації співробітників або клієнтів і надання їм фізичного доступу до захищеного офісу або серверної кімнати.

Одним із найпоширеніших застосувань штучного інтелекту в біометричних даних є розпізнавання облич. Хоча в деяких випадках просте розпізнавання обличчя може спрацювати для точної ідентифікації людей, воно схильне до деяких недоліків. Сюди входять відмінності в освітленні, в тому числі в залежності від пори року, низька продуктивність через расові упередження та вразливість до хибно-позитивних атак, як, наприклад, звичайне використання зображення перевіреної особи, яка має доступ до захищених об’єктів [27].

Однак і ці недоліки можна пом’якшити, для того, щоб допомогти визначити дійсних користувачів і підвищити продуктивність у різних умовах. У випадку з розпізнаванням облич, вже є багато варіантів попередньо навчених моделей виявлення обличчя, проте, очевидно, це теж вимагатиме додаткових ресурсів для здійснення розрахунків та прогнозів.

Ще одним популярним використанням біометричних даних є розпізнавання голосу. Подібно до того, як певне зображення особи може бути представлено у вигляді пікселів і проаналізовано комп’ютером, голосові записи також можна моделювати в цифровому вигляді. Це також відкриває багато переваг, які надає розпізнавання обличчя в тих місцях, де доступ до камери може бути недоступний. Наприклад, підтвердження особи клієнта по телефону за допомогою служби автоматичного автовідповідача. Його також можна використовувати для виявлення порушень працездатності у осіб, що звертаються до правоохоронних органів

заявляючи, наприклад, про замінування станцій метро, будівель навчальних закладів, чи інших публічних місць. Проте ризики застосування розпізнавання голосу для контролю доступу все ще залишаються досить високими, оскільки комп’ютерні системи, як і живі люди, можуть з великою ймовірністю переплутати потрібну особу із вмілим пародистом, якщо вони будуть орієнтуватись лише тільки на голос.

Очевидно, що фізична безпека може бути заснована на набагато більшому, ніж просто на розпізнаванні голосу чи обличчя. Дослідники з Китаю змогли успішно ідентифікувати суб'єктів на основі їхньої ходи. Аналізуючи різні рухи в силуеті людини, вони змогли моделювати унікальні пози. Їхня модель змогла обробити годину відео всього за 10 хвилин [28].

Сканер венозного малюнку долоні відноситься до біометричного пристрою аутентифікації, який використовується для сканування візерунків вен на долоні особи для аутентифікації особи. Він використовує інфрачервоне світло для захоплення зображення візерунків, розташованих під шкірою. Ця технологія працює за принципом порівняння та аутентифікації збереженого шаблону вен у базах даних із візерунком вен, наявним на долоні особи, що забезпечує високий рівень точності для розпізнавання особистості цієї особи.

Зростаюча потреба в захисті конфіденційної інформації привертає увагу кількох бізнес-організацій, щоб включити сканери вен долоні в свої організації, що призведе до глобального сплеску зростання ринку, оскільки ці сканери забезпечують ідеальну безпеку, точність, надійність, простоту використання тощо.

Завдяки цифровізації зростає кількість випадків шахрайства та злочинів в Інтернеті, що становить загрозу безпеці. Кіберзлочини, крадіжки, злом, шахрайство тощо змушують державний, а також приватний сектори зберігати та використовувати сканери вен долоні для точної аутентифікації особи користувачів та запобігання таким видам шахрайства.

Ініціативи уряду із заохочення впровадження новітніх технологій, таких як біометричні сканери вен долоні, стимулюють попит на ці сканери. Уряд сам використовує цю технологію для отримання дозволів на проживання, аутентифікації

паспортів, національної реєстрації тощо, щоб ідентифікувати громадян та уникнути шахрайства.

Використання моделей штучного інтелекту для забезпечення біометричної безпеки збільшує здатність біометричного програмного забезпечення виявляти унікальні фізичні маркери, такі як голос, обличчя, стійка чи хода. Крім того, деякі моделі тепер можуть виявляти поведінкові біометричні ознаки, а також використовуватись для постійного моніторингу поведінки користувачів. Ці переваги стимулюють корпоративне впровадження біометричних даних і допомагають стимулювати подальше зростання технології, оскільки вона сприяє безпеці підприємства.

Біометричні рішення самі по собі зазвичай є досить складними, але інколи обґрунтованим та потрібним ускладненням є додатковий рівень рішень на основі штучного інтелекту, який підвищує ефективність цієї технології. Ці технічні рішення мають вирішальне значення для захисту корпоративних даних у все більш цифровому світі, та можуть допомогти захистити фізичні активи бізнесу. Відповідальними за прийняття таких рішень є самі компанії та їх керівники з безпеки, адже аналіз ризиків є важливою складовою перед прийняттям рішення про використання більш простого та дешевшого рішення, чи такого, яке потребує більше коштів, уваги співробітників та ресурсів на додаткову обробку інформації.

Саме використання біометричних технологій сприяє розвитку безпеки організації в цілому, та може стати рушієм важливих змін в організації контролю доступу.

3.2 Аналіз показників ефективності СКУД із біометричними даними

Оскільки здатність сканерів виявляти фальсифіковані біометричні дані покращується, зловмисники також будуть наполегливо працювати над створенням кращих підробок та способів обходу захисту.

Біометричні дані будуть найефективнішими, якщо використовувати їх у поєднанні зі стратегією багатофакторної аутентифікації (MFA).

Поки датчики та сканери не зможуть краще виявляти відхилення чи фальшиві дані, біометричні дані завжди повинні бути одним із компонентів багатофакторної системи аутентифікації, тому що кілька етапів процесу добре доповнюють один одного. Зловмисники шукають найпростіші шляхи проникнення, тому додаткові шари захисту з досить високою ймовірністю змусить зловмисника відмовитись від своїх планів.

Також при цьому всі біометричні дані повинні бути збереженими виключно на безпечних і зашифрованих серверах і в хмарних середовищах.

Обов'язковою є обробка біометричних даних з такою ж обережністю, як і обробка будь-якої іншої особистої інформації, яку контролює компанія. Також при впроваджених біометричних технологіях важливо також слідкувати за наявними та свіжими законами, що регулюють біометричні дані.

На сьогодні існує два способи ідентифікації людини по долоні – за формою та за термограмою вен [29].

Ідентифікація на основі геометрії долоні – цей метод засновано на розпізнаванні геометричних особливостей долоні. Спеціальний пристрій формує тривимірне зображення кисті руки, який потім перетворюється на згортку. Сьогодні цей метод ідентифікації користувачів за геометрією руки не так розповсюджений як за відбитками пальців, але теж використовується.

Переваги ідентифікації за геометрією долоні порівняно з плюсами ідентифікації за відбитками пальців у питанні надійності, хоча пристрій для зчитування відбитків долонь займає більше місця [29].

Другий спосіб ідентифікації – це використання термограми розташування вен долоні. Сам спосіб засновано на тому ефекті, що вени долоні виділяють тепло, тому можливо отримати зображення їх розташування за допомогою інфрачервоної камери та на основі отриманого зображення проводити ідентифікацію. Цей спосіб дуже надійний, проте не досить розповсюджений, бо ще не існує чітких алгоритмів його функціонування [29].

Розглянемо детальніше процес сканування венозного малюнку долоні. Процес сканування вен на долоні використовує світло близького до інфрачервоного

випромінювання для освітлення вен руки та потоків венозної крові, які є унікальними для кожної людини. Такий процес є швидким, а ідентифікація точною. Сканування не потребує безпосереднього контакту руки із поверхнею сканера, але сканер також легко дезінфікується антибактеріальними серветками у випадках, якщо користувачам таки захочеться безпосередньо доторкатись до сканера.

Сканер вен на долоні відноситься до біометричного пристрою аутентифікації, який використовується для сканування візерунків вен на долоні особи для аутентифікації особи. Він використовує інфрачервоне світло для захоплення зображення візерунків, розташованих під шкірою. Ця технологія працює за принципом порівняння та аутентифікації збереженого шаблону вен у базах даних із візерунком вен, наявним на долоні особи, що забезпечує високий рівень точності для розпізнавання особистості цієї особи.

Схематично процес зображено на рисунку 3.1 [30]:

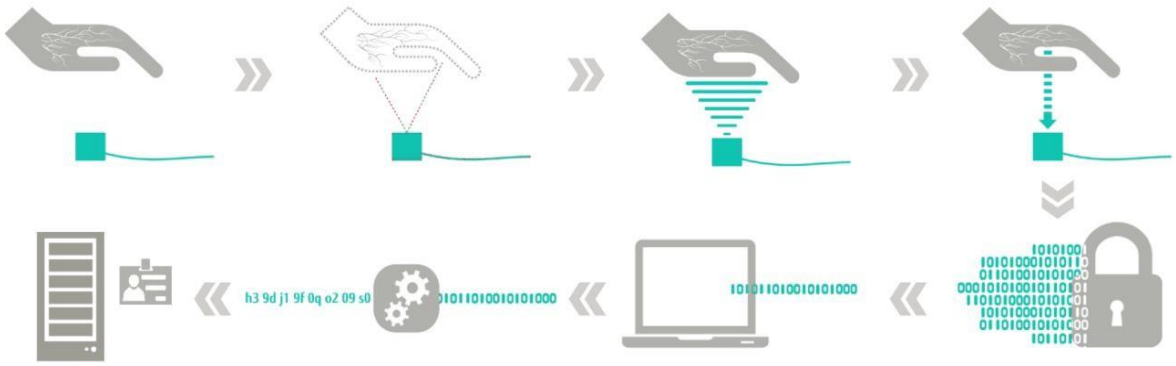

Рисунок 3.1 – Процес аутентифікації за допомогою сканера венозного малюнка долоні

Дані зі сканування шифруються і зберігаються в базі даних. База даних може зберігати також будь-яку потрібну додаткову інформацію, проте основною частиною, яка призначена саме для здійснення однозначної ідентифікації користувачів, має бути відповідний біометричних ідентифікатор в зашифрованому вигляді.

Ринок сканерів вен долоні набирає обертів через зростання потреби в цілях безпеки в приватному та державному секторах. Сканери вен на долоні

використовуються в ряді секторів, включаючи сектори охорони здоров’я, банківський сектор, бізнес-організації, військовий та оборонний сектори тощо, що призводить до високих інвестицій на цьому ринку.

Очікується, що ринок сканерів долонних вен зростатиме вражаючими темпами в усьому світі через зростаючу державну підтримку та ініціативи в цілях безпеки та безпеки. За оцінками, до 2030 року буде спостерігатися стабільний CAGR(Сукупний середньорічний темп росту) галузі.

Висновки за розділом 3

Новітні біометричні технології та їх використання в системах контролю управління доступом є хорошим показником того, що організаціям, які їх використовують, важлива безпека як співробітників та персоналу, так і фізичних активів компанії, які можуть розташовуватися в приміщенні компанії.

Якщо колись додаткові технології використовувались лише для доступу до окремих приміщень чи особливо важливих зон наприклад в дослідних центрах, лабораторіях, банках, то на теперішній час їх використання набуло значно ширшого поширення для організації обмеженого доступу до інформації, наприклад до медичних даних чи даних судових реєстрів.

Новітні технології можуть бути використані для ідентифікації особи для надання їх певних персоніфікованих послуг, соціальних, медичних, фінансових, страхових та інших сервісів. Ну і само собою без додаткових перевірок не може бути проведена точна ідентифікація особи, яка відповідальна за управління процесами та прийняття рішень, наслідки яких можуть мати критичне значення, якщо вони стосуються органів державної влади, оборонних відомств, чи, наприклад, керування енергоблоками на атомних станціях.

РОЗДІЛ 4
ВИКОРИСТАННЯ НОВІТНІХ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ В ДВОФАКТОРНІЙ АУТЕНТИФІКАЦІЇ

4.1 Аналіз варіантів поєднань кількох факторів

Майбутнє технологій безпеки знаходиться в руках хмарних рішень і розумних проектів, які можуть безперешкодно інтегруватися один з одним для створення уніфікованих систем безпеки, які є більш безпечними, ніж це вважалося можливим.

Об’єднання біометричних технологій із рішеннями безпеки доступу є одним із перших важливих кроків у напрямі високоінтегрованого технологічного рішення, і починає здаватися, що можливості для подальшого просування безмежні.

Зазвичай достатньою інформацією для входу був один з факторів:

- Що ти знаєш?
- Що ти маєш?
- Ким ти є?

Але вже при поєднанні декількох видів унікальних даних – отримуємо багатофакторну аутентифікацію, яка може поєднати в собі будь-які два, або й всі три типи ідентифікаторів, як зображено на рисунку 4.1 [31].

Ще донедавна такий високий рівень безпеки обмежувався деякими користувачами вищого ешелону, такими як керівники компаній, IT-адміністратори, високопоставлені державотворці або інші, чия інформація та доступ вважалися надважливими. Наприклад, генеральному директору, можливо, доведеться як пред’явити картку, так і ввести код доступу, або використати відбиток пальця чи сканер венозного малюнку долоні, щоб відкрити двері до кабінету, де міститься багато речей із обмеженим доступом. А робочий стіл, яким користується керівник відділу IT, може бути захищений і паролем, і свайпом карти доступу на допоміжному зчитувачі, підключеному до комп’ютера.

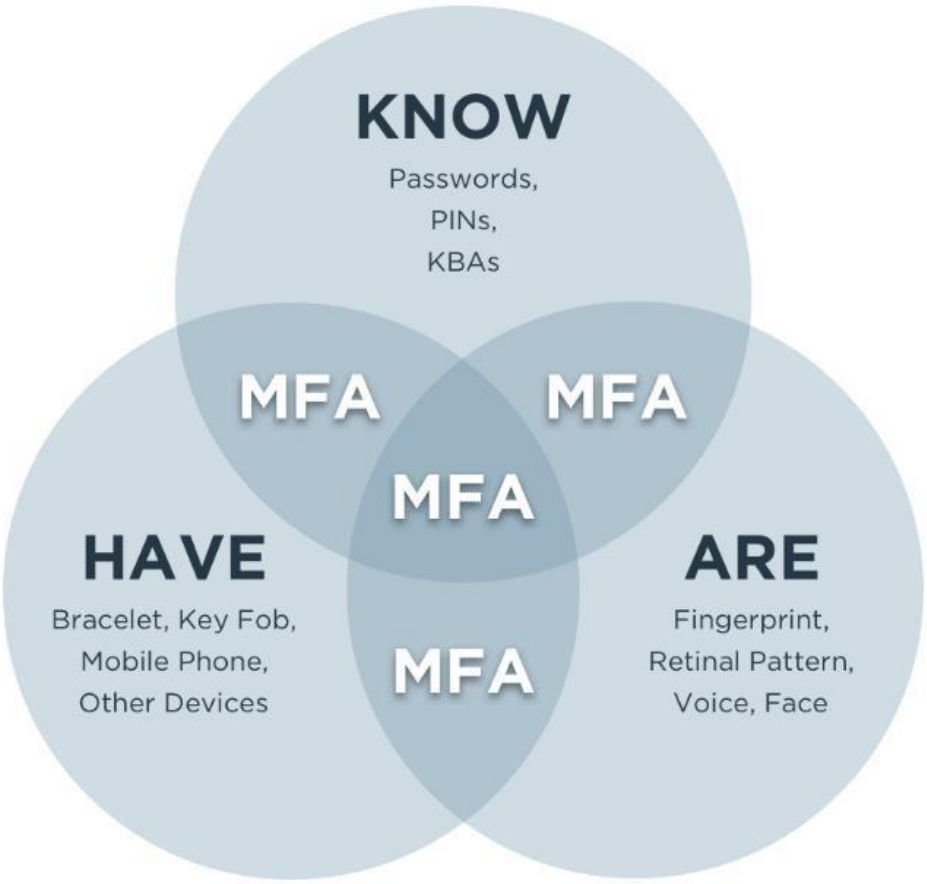

Рисунок 4.1 – Дані при мультифакторній аутентифікації

Вартість і складність впровадження технології багатофакторної аутентифікації в минулому вважалися основними причинами, щоб обмежити використання додаткових гарантій невеликим відсотком корпоративного персоналу, але ці аргументи все частіше залишаються осторонь, оскільки впровадження рішень стає простішим, а ціни – нижчими.

Інтегратори систем безпеки вже стабільно встановлюють системи контролю доступу на основі карток, то чому б не попрацювати з наявними обліковими даними та додати до них рівень логічного доступу?

Мобільність звичайного користувача, який бере свій ноутбук додому на вихідних або подорожує у справах, робить більш значущим наявність принаймні двофакторної аутентифікації для додаткової логічної безпеки. Те ж саме стосується захисту певних фізичних активів або територій, таких як лікарняна шафа з ліками

або кімната записів у фінансовій установі. Встановлення систем, що вимагають багатофакторної аутентифікації, може запобігти дорогим або навіть нормативним помилкам у цих ключових областях.

Працюючи в партнерстві, інтегратори, персонал фізичної безпеки та IT-відділ можуть використати інвестиції в систему фізичного контролю доступу в систему, яка забезпечує більш високий рівень безпеки, використовуючи також логічну сторону. Це дійсно той випадок, коли один спосіб аутентифікації вже є хорошим, але два – значно кращими в зв’язці.

Поєднання біометричної ідентифікації особи із другим фактором для входу може вирішити декілька потенційних проблем, пов’язаних із вразливістю різних технологій поодинці. Лише в зв’язці вже звичного способу фізичної аутентифікації з іншим фактором, який використовує новітні біометричні технології, а саме сканер венозного малюнку долоні, таке рішення може стати надійним та безпроблемним для організації.

Будь-яка СКУД має свої обмеження за кількістю користувачів, тому при виборі систем контролю доступу важливо забезпечити відповідність перспективним планам розвитку.

Оптимальним рішенням послужить установка системи з можливістю простої та швидкої модернізації, зводячи втрати з «нарощування» системи до мінімуму, додаючи потрібні модулі (модульність).

При проектуванні систем контролю та керування доступом необхідно закладати можливість інтегруватись з іншими системами безпеки.

Розглянемо основні критерії біометричної ідентифікації [32]:

FAR (False Acceptance Rate) - коефіцієнт хибного пропуску.

FRR (False Rejection Rate) - коефіцієнт хибної відмови.

Характеристики FAR, FRR отримують розрахунковим шляхом на основі методів математичної статистики. Чим нижче ці показники, тим точніше розпізнавання об'єкта. Сукупність наступних факторів є значущою для порівняння різних біометричних технологій [32]:

• стійкість до фальсифікації даних;

• можливість строгої аутентифікації;

• незмінність біометричних характеристик;

• чутливість до зовнішніх факторів;

• швидкість аутентифікації;

• можливість безконтактної аутентифікації;

• психологічний комфорт користувача;

• вартість реалізації біометричних методів СКУД.

Детальніше показники наведені у таблиці 4.1.

Для ідентифікації особи та подальшої її аутентифікації може використовуватись термінал двофакторного контролю доступу, який містить в собі:

- сканер венозного малюнку долоні;
- зчитувач безконтактних / smart карток.

Таблиця 4.1

Показники FAR та FRR для різних біометричних технологій в СКУД

Біометрична технологія в СКУД	**FAR**	**FRR**
Відбиток пальця	0,001%	0,6%
Розпізнавання обличчя 2D	0,1%	2,5%
Розпізнавання обличчя 3D	0,0005%	0,1%
Райдужна оболонка ока	0,00001%	0,016%
Сітківка ока	0,0001%	0,4%
Малюнок вен долоні	0,00008%	0,01%

Окрім вже згаданих вище факторів, важливими з точки зору безпеки також є можливість підробки біометричного ідентифікатора, чи підходить він для строгої аутентифікації, та якою є незмінність характеристики та чутливість до зовнішніх факторів.

Для безпосереднього користувача важливими факторами є лише швидкість аутентифікації та особистий комфорт, адже цікавість до новинки швидко спадає, а проблематичний або надто довгий процес аутентифікації перед входом в захищену зону швидко починає дратувати.

Щодо власників, то їх від впровадження нових технологій найчастіше зупиняє їх вартість, тому саме вартість реалізації може також стати вирішальною складовою при виборі технології до впровадження.

Зведені фактори для різних біометричних технологій наведені у таблиці 4.2.

Таблиця 4.2

Значущі фактори для порівняння біометричних технологій в СКУД

Біометрична технологія в СКУД	**FAR,%**	**FRR,%**	**Підробка**	**Строга аутенти-фікація**	**Незмінність характеристики**	**Чутливість до зовнішніх факторів**	**Швидкість аутенти-фікації**	**Комфорт користувача**	**Вартість реалізації**
Відбиток пальця	0,001	0,6	Можлива	Можлива	Низька	Висока	Висока	Середній	Низька
Розпізнавання обличчя 2D	0,1	2,5	Можлива	Ні	Низька	Висока	Середня	Високий	Середня
Розпізнавання обличчя 3D	0,0005	0,1	Проблематична	Ні	Висока	Низька	Низька	Середній	Висока
Райдужна оболонка ока	0,00001	0,016	Неможлива	Можлива	Висока	Середня	Висока	Високий	Висока
Сітківка ока	0,0001	0,4	Неможлива	Можлива	Середня	Висока	Низька	Низький	Висока
Малюнок вен долоні	0,00008	0,01	Неможлива	Можлива	Середня	Середня	Висока	Середній	Середня

Сучасні рішення дозволяють суміщати спеціальні біометричні сканери з стандартними системами пропуску. Спеціальний термінал може одночасно містити як сканер венозного малюнку долоні, так і зчитувач електронної ключ-карти. При двофакторній аутентифікації важливим є співпадіння особи по обох факторах, і лише після цього буде надано дозвіл на вхід.

Супутнє до такого терміналу програмне забезпечення (ПЗ) може додатково містити наступні функції [33]:

- Повнофункціональний автономний режим роботи пристроїв.
- Аутентифікація з декількома обліковими записами.
- Моніторинг у реальному часі.
- Інтуїтивно зрозумілі карти.
- Повна інтеграція між модулями.
- Керування обмеженнями.

- Логіни та керування ролями.
- API для легкої інтеграції.
- Мобільний додаток.

Дані пункти є опціональними і можуть бути реалізовані або увімкнені в залежності від потреб організації та можливостей обраного постачальника таких пристроїв.

На рисунку 4.2 зображено схему отримання доступу з використанням біометричних даних.

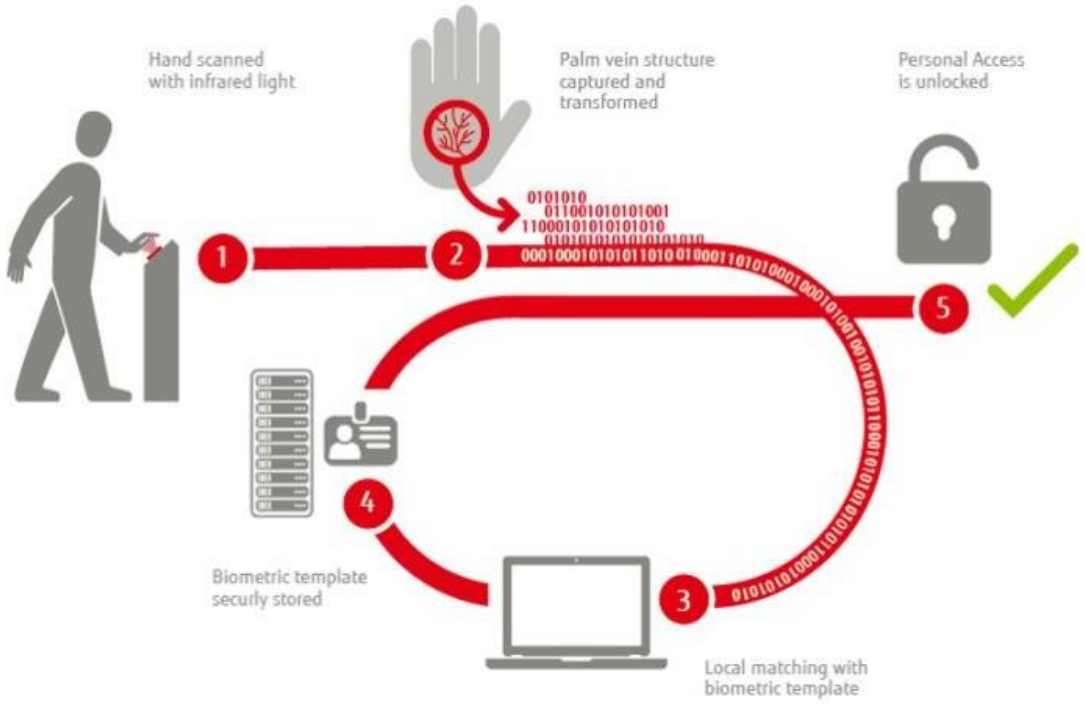

Рисунок 4.2 – Схема отримання доступу з використанням біометричних даних

Таким чином, при використанні терміналів з підтримкою декількох способів аутентифікації особи, вхід для безпосереднього користувача буде відбуватись швидко та зручно, що також не дозволить утворитись великим чергам з бажаючих потрапити в будівлю чи на територію захищеного об’єкта.

4.2 Перспективи застосування пропонованого рішення на практиці

Проблеми фізичної безпеки та контролю доступу залишається актуальними не зважаючи на перехід багатьох компаній на гібридний або частково віддалений формат роботи у зв’язку з пандемією та війною, яка принесла за собою масові релокації співробітників компаній, які мають змогу здійснювати свою діяльність відділено.

Стандартні, давно відомі системи контролю управління доступом мають ряд переваг та підкупають своєю зручністю, але в той же час залишають досить великі ризики із несанкціонованого доступу, доступу сторонніми особами за допомогою вкраденої інформації, карточки, бейджа.

Помічними для однозначної ідентифікації особи є біометричні технології, які вже широко використовуються в СКУД обладнаних сканерами відбитків пальців, сканерами венозного малюнку долоні, сканерами сітківки ока та багатьма іншими. Точність такої ідентифікації є досить високою та суттєво знижує ризики, які присутні при використанні стандартних СКУД.

На основі дослідженої інформації визначено, що оптимальним з точки зору зручності та аналізу ризиків варіантом є поєднання стандартного способу контролю управління доступом наприклад у вигляді електронної карточки чи її цифрової копії в телефоні співробітника із другим фактором, який використовуватиме новітні біометричні технології для підвищення точності ідентифікації та зменшення ризиків несанкціонованого доступу настільки це можливо.

Висновки за розділом 4

В даному розділі було запропоновано вирішення проблеми підвищення ефективності систем контролю управління доступом за рахунок використання не лише новітніх біометричних показників, але й за рахунок їх використання при двофакторній аутентифікації.

Біометричні рішення є досить хорошим способом підвищення рівня захищеності, проте для уникнення неприємних несподіванок у вигляді навмисного чи випадкового надання доступу стороннім особам, було розглянуто систему із вже давно звичного всім ключа-карти (фактор – «Що я маю?») та ідентифікатора венозного малюнку долоні (фактор – «Ким я є?»), який є для кожної особи унікальним, та неможливим для підробки.

ВИСНОВКИ

В роботі виконано поставлені перед її початком задачі, проаналізовано існуючі підходи до організації контролю доступу, проаналізовано процес розвитку СКУД для кращого розуміння початкових потреб та передумов виникнення систем захисту, зібрано та проаналізовано вхідні дані для їх використання в моделюванні системи СКУД із використанням біометричного фактору, запропоновано модель поєднання двох факторів для підвищення ефективності систем контролю управління доступом та уникнення потенційних ризиків при використанні лише одного з факторів.

Так як раніше і справді підвищені заходи безпеки та засоби що їх гарантують бути надзвичайно дорогими та складними в експлуатації, та були доступними лише для привілейованого кола осіб та для керівництва деяких компаній, то зараз ситуація змінилась на користь усіх гравців ринку та потенційних споживачів новітніх технологій із числа компаній та організацій різного розміру та форми власності.

Запропоновані рішення можуть бути застосовані в організаціях різного спрямування, зокрема в охоронних та силових структурах, органах державної та виконавчої влади, на митниці, в прикордонній та міграційній службах, на об’єктах критичної інфраструктури та підприємствах, які потребують підвищеного рівня організації безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ilic-Godfrey, S. Artificial intelligence: taking on a bigger role in our future security [Електронний ресурс], Ilic-Godfrey Stanislava – 2021. – Режим доступу до ресурсу: https://www.bls.gov/opub/btn/volume-10/investigation-and-security-services.htm.

2. Steve K. COVID-19 Put These Access Control Solutions in the Spotlight [Електронний ресурс], Karantzoulidis Steve. – 2022. – Режим доступу до ресурсу: https://www.securitysales.com/access/covid-19-access-control-spotlight/.

3. Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Smart environment as a service: three factor cloud based user authentication for telecare medical information system," Journal of Medical Systems, vol. 38, article no. 9997, 2014.

4. Axis Communications. Cloud technology in end-to-end surveillance solutions [Електронний ресурс] , Axis Communications. – 2021. – Режим доступу до ресурсу: https://www.axis.com/en-no/newsroom/article/cloud-end-to-end.

5. Malik, A. RTLS for Dummies. Wiley, 336p., 2009.

6. Zhang, C., Hammad, A., Soltani, M., Setayeshgar, S., & Motamedi, A. Dynamic virtual fences for improving workers safety using BIM and RTLS. In Proceedings of the 14th International Conference on Computing in Civil and Building Engineering, June, 2012.

7. Kamala Kannan, T., Sharmila, K., Shanthi, M. C., & Devi, M. R. Study on Cloud Storage and its Issues in Cloud Computing. International Journal of Management, Technology And Engineering, 9(1), 2019.

8. Carlaw S., Impact on biometrics of Covid-19. Biometric Technology Today, 2020(4), 8-9, 2020.

9. Shankar, K. The impact of COVID- 19 on IT services industry- expected transformations. British Journal of Management, 31(3), 450, 2020.

10. Захаров В.П., Рудешко В.І. Використання біометричних технологій правоохоронними органами у XXI столітті: науково-практичний посібник, В.П. Захаров, В.І. Рудешко. - Львів: ЛьвДУВС, 2009. - 440с.

11. The History of Access Control [Електронний ресурс]. –Режим доступу до ресурсу: https://www.grosvenortechnology.com/2021/08/the-history-of-access-control/.

12. Jajodia, S., Samarati, P., Sapino, M. L., & Subrahmanian, V. S. Flexible support for multiple access control policies. ACM Transactions on Database Systems (TODS), 26(2), 214-260, 2001.

13. Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. Role-based access control. Artech house, 2003.

14. Fennelly, L. J., & Perry, M. A. The Four Basic Layers of Physical Security. In CPTED and Traditional Security Countermeasures150 Things You Should Know (pp. 36-37). CRC Press, 2018.

15. Купін, А. І., & Кумченко, Ю. О. Аналіз існуючих підходів біометричної ідентифікації та аутентифікації людини. Системні технології, (4), 129-134, 2013.

16. Царенко, В. В. Системи контролю і управління доступом до об’єктів, що охороняються, 2020.

17. Pal, S., Dorri, A., & Jurdak, R. Blockchain for IoT access control: Recent trends and future research directions. Journal of Network and Computer Applications, 103371, 2022.

18. The 2020 State Of Physical Access Control Report [Електронний ресурс]. – Режим доступу до ресурсу: https://www.hidglobal.com/doclib/files/resource_files/hid-pacs-2020-state-physical-access-wp-en.pdf.

19. Unar, J. A., Seng, W. C., & Abbasi, A. A review of biometric technology along with trends and prospects. Pattern recognition, 47(8), 2673-2688, 2014.

20. Khanday, A. M. U. D., Amin, A., Manzoor, I., & Bashir, R. Face recognition techniques: a critical review. STM Journals [Internet], 5(2), 24-30, 2018.

21. Zahrouni, L., Blackwood, D., Rizvi, S., Gualdoni, J., & Almiani, M. Preventing identity theft using biometrics based authentication system. In 2017 IEEE

jordan conference on applied electrical engineering and computing technologies (AEECT) (pp. 1-6). IEEE, 2017.

22. Komoldinovich, A. J. Intelligent System for Information Security Management: Architecture and Design Problems. European Multidisciplinary Journal of Modern Science, 5, 383-397, 2022.

23. Zahid, Z., Haider, A., Sabahat, N., & Tanwir, A. Vulnerabilities in Biometric Authentication of Smartphones. In 2020 IEEE 23rd International Multitopic Conference (INMIC) (pp. 1-5). IEEE, 2020.

24. Lei, X., Tu, G. H., Liu, A. X., Li, C. Y., & Xie, T. The insecurity of home digital voice assistants-vulnerabilities, attacks and countermeasures. In 2018 IEEE Conference on Communications and Network Security (CNS) (pp. 1-9). IEEE, 2018.

25. Won, Y. G., Bae, T. M., & Ro, Y. M. Scalable protection and access control in full scalable video coding. In International Workshop on Digital Watermarking (pp. 407-421). Springer, Berlin, Heidelberg, 2006.

26. Gofman, M., Mitra, S., Tadesse, B., & Villa, M. Biometrics for Enterprise Security Risk Mitigation. In Advances in Cybersecurity Management (pp. 163-195). Springer, Cham, 2021.

27. Jaswal, G., Kanhangad, V., & Ramachandra, R. (Eds.). AI and Deep Learning in Biometric Security: Trends, Potential, and Challenges. CRC Press, 2021.

28. IEEE Transactions on Pattern Analysis and Machine Intelligence 25(12):1505- 1518, 2004.

29. Michael, G. K. O., Connie, T., & Teoh, A. B. J. A contactless biometric system using palm print and palm vein features. Advanced Biometric Technologies, 155-177, 2011.

30. CPNI Biometric Authentication in Automatic Access Control Systems [Електронний ресурс], Режим доступу до ресурсу: https://media-exp1.licdn.com/dms/document/C4E1FAQH-D8tbKXCD3w/....

31. Zain M. 8 Benefits of Multi-Factor Authentication (MFA) [Електронний ресурс] / Zain Malik. – 2022. – Режим доступу до ресурсу: https://www.pingidentity.com/en/resources/blog/post/eight-benefits-mfa.html.

32. Wayman, J., Jain, A., Maltoni, D., & Maio, D. An introduction to biometric authentication systems. In Biometric Systems (pp. 1-20). Springer, London, 2005.

33. Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих навчальних Ц18 закладів], Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.: іл.

34. Цирульник С.М., Перевозніков С.І., Озеранський, В.С. Автоматизація проектування мікропроцесорних систем контролю доступу та охорони. Вісник Вінницького політехнічного інституту, 2009, 10-14.

35. Царенко, В.В. Системи контролю і управління доступом до об’єктів, що охороняються, 2020, 82.

36. Баглай, Р.О. Загрози безпеки хмарних технологій для банків. Системи обробки інформації, 2018, 1: 127-135.

37. Ільїн, О.О., Сєрих, С.О., Вишнівський, В.В. Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки. Сучасний захист інформації, 2017, 1: 66-72.

38. Новіцький, Г.М. Метод розпізнавання рисунка вен долоні за ключовими точками. Хмельницького національного університету, 2019, 92.

39. A guide to biometrics / RM Ball Jonathan X Connell, Sharath Pankanti et al .; trans. with English. N. E. Agapova. - M .: Technosphere, 2007. - 367 p.

40. Markelov KS Identification and verification of personality - a complex biometric information technology / International Jornal of Open information Technologies ISSN: 2307-8162, vol. 3, no 5, 2015, p.12-18.

41. Мороз, А.О. Біометричні технології ідентифікації людини. Огляд систем. Математические машины и системы, 2011, 1.1: 39-45.

42. Fennelly, Lawrence J. (ed.). Effective physical security. Butterworth-Heinemann, 2016. - 458 p.

43. Saini, Rupinder, Rana, Narinder. Comparison of various biometric methods. International Journal of Advances in Science and Technology, 2014, 2.1: 24-30.

44. Michael, Goh Kah Ong, Tee Connie, and Andrew Beng Jin Teoh. "Touch-less palm print biometrics: Novel design and implementation." Image and vision computing 26.12 (2008): 1551-1560.

45. Наконечний В.С., Кулеша Г.А. Новітні біометричні технології в системах контролю управління доступом. V Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS) 2022, КИЇВ, Україна.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Тези наукових доповідей:

1. Наконечний В.С., Кулеша Г.А. Новітні біометричні технології в системах контролю управління доступом. V Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS) 27 - 28 ЖОВТНЯ 2022, КИЇВ, Україна