

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКРОСЬКОГО»

Факультет електроніки

(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем

(повна назва кафедри)

«На правах рукопису»
УДК 621.391.83:681.518

«До захисту допущено»

Завідувач кафедри



С.А. Найда

(ініціали, прізвище)

15

грудня 2022 р.

Магістерська дисертація

зі спеціальності 171 Електроніка

(код і назва)

на тему: Особливості сучасного апаратного забезпечення безпроводових систем безпеки

Виконав: студент II курсу, групи ДВ-11мп

(шифр групи)

Горєв Олександр Володимирович

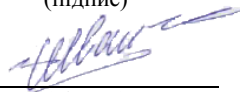
(прізвище, ім'я, по-батькові)



(підпис)

Керівник доц. каф. АМЕС, к.т.н., доц. Швайченко В.Б.

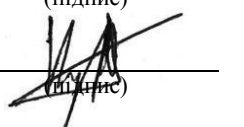
(посада, науковий ступінь, вчене звання, прізвище та ініціали)



(підпис)

Рецензент проф. каф. ЕПС, д.т.н., проф. Кузьмичєв А.І.

(посада, науковий ступінь, вчене звання, прізвище та ініціали)



(підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.

Студент


(підпис)

**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**

Факультет електроніки

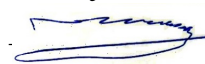
Кафедра акустичних та мультимедійних електронних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою Електронні системи мультимедіа та засоби Інтернету речей

Спеціальність 171 Електроніка
(спеціалізація))

ЗАТВЕРДЖУЮ

Завідувач кафедри



С.А. Найда
(ініціали, прізвище)

« 01 » 09 2022 р.

**ЗАВДАННЯ
на магістерську дисертацію студенту**

Горєву Олександрову Володимировичу

(прізвище, ім'я, по-батькові)

1. Тема роботи Особливості сучасного апаратного забезпечення безпроводових систем безпеки

Керівник роботи Швайченко Володимир Борисович, доцент, к.т.н.
(прізвище, ім'я, по-батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «08» листопада 2022 р. №4092-с

2. Строк подання студентом дисертації 19 грудня 2022 р.

3. Об'єкт дослідження: Процеси в сучасних безпроводових системах безпеки що визначають їх переваги та недоліки, способи передачі контенту.

4. Предмет дослідження: Апаратно – програмне забезпечення безпроводових систем безпеки.

5. Перелік завдань, які потрібно розробити:

Аналіз ринку систем безпеки, визначення переваг і недоліків БСБ, аналіз

протоколів передачі інформації, дослідження передачі інформації. розробки стартап-проекту.

6. Перелік графічного (ілюстративного) матеріалу: 15 слайдів презентації,

7. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

8. Дата видачі завдання 01 вересня 2022 р.

Календарний план

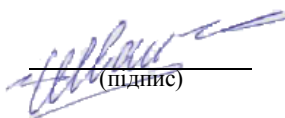
№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів роботи	Примітка
1	Написання першого розділу	15.10.2022	виконано
2	Написання другого розділу	29.10.2022	виконано
3	Написання третього розділу	30.11.2022	виконано
4	Написання четвертого розділу	05.12.2022	виконано
5	Підготовка матеріалів до друку та оформлення пояснювальної записки	10.12.2022	виконано
6	Підготовка та оформлення презентації для доповіді	18.12.2022	виконано

Студент


(підпис)

Горєв О.В.
(ініціали, прізвище)

Керівник


(підпис)

Швайченко В.Б.
(ініціали, прізвище)

УДК 621.391.83:681.518

РЕФЕРАТ

Горєв О.В. Особливості сучасного апаратного забезпечення безпроводових систем безпеки: магістерська дисертація: 171 Електроніка / Горєв Олександр Володимирович. – Київ, 2022. – 88 с.

Ключові слова: система безпеки, протокол, AJAX Systems, відео, IP камера.

Актуальність роботи. Дослідження безпроводових систем безпеки є актуальним, так як ця технологія є відносно новою, і покращення процесів передавання інформації та підвищення безпеки цих, як в межах самої системи, так і для передачі певної інформації в централі прийняття рішень є досить важливими. Все більше людей надають перевагу саме безпроводовим системам, так як це візуально краще оформлений продукт, є більш зручним у використанні та встановленні.

Мета і завдання дослідження. Метою роботи є дослідження сучасних безпроводових систем безпеки, виявлення наявних переваг та недоліків та спроба покращити результати на користь вибору саме БСБ для конкретного застосування.

Завдання дослідження:

- проаналізувати ринок систем безпеки;
- проаналізувати переваги та недоліки безпроводових систем безпеки;
- проаналізувати протоколи передачі даних в БСБ;
- визначити варіанти збурень і способи їх уникнень;
- виконати дослідження на рівні протоколів передачі інформації з метою покращення процесу;
- розробити стартап-проект бюджетної компанії безпроводових охоронних систем.

Об’єкт дослідження. Процеси в сучасних безпроводових систем безпеки, що визначають їх переваги та недоліки, способи передачі контенту.

Актуальність створення стартапу, який націлений на продаж, пов'язана з встановленням та обслуговуванням безпроводових систем безпеки.

Предмет дослідження. Апаратно – програмне забезпечення безпроводових систем безпеки, протоколи передавання інформації

Методи дослідження. Аналіз світового ринку та ринку України наявних фірм по виготовленню безпроводових систем безпеки, дослідження актуальних протоколів передавання інформації через сучасне програмне забезпечення і програмування.

Наукова новизна одержаних результатів. Покращення протоколу передачі RTP для підвищення якості передавання інформації та уникнення підробки відеоданих.

Практичне значення одержаних результатів. Результати дослідження, наведені в даній магістерській дисертації можна використовувати для аналізу безпроводових систем безпеки, їх комбінування і цілісного розуміння вартості, переваг та недоліків їх використання. Досліджений алгоритм передавання інформації можна використовувати в нових розробках IP камер і технологій, що працюють через протоколи передавання відеоданих.

ABSTRACT

*Gorev O.V. Features of modern hardware for wireless security systems:
Master's thesis: 171 Electronics / Gorev Oleksandr V. - Kyiv, 2022. - 88 p.*

Keywords: security system, protocol, AJAX Systems, video, IP camera.

Relevance of the work. The study of wireless security systems is relevant, as this technology is relatively new, and there are many points on which it is possible to study and improve the processes of information transfer, both within the system itself and to transfer certain information to the decision-making center. More and more people prefer wireless systems, as it is a visually better designed product, more convenient to use and install.

The purpose and objectives of the study. The aim of the study is to investigate modern wireless security systems, to find their pros and cons and to try to improve the results in favor of choosing the BSB.

The objectives of the study:

- to analyze the market of security systems;
- to analyze the advantages and disadvantages of wireless security systems;
- to analyze the data transmission protocols in the BSB;
- to identify options for disturbances and ways to avoid them;
- to perform research at the level of information transfer protocols in order to improve the process;
- to develop a startup project of a budget company of wireless security systems.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	9
ВСТУП.....	11
1. СТАН СУЧАСНИХ БЕЗПРОВОДОВИХ СИСТЕМ БЕЗПЕКИ.....	12
1.1 Аналіз особливостей сучасних безпроводових систем безпеки.	12
1.2. Порівняння застосовних безпроводових технологій в системах безпеки.	22
1.3 Стан апаратного забезпечення безпроводових систем безпеки.....	32
Висновки до розділу	40
2. ВИЗНАЧЕННЯ ФАКТОРІВ ВПЛИВУ НА БЕЗПРОВОДОВІ КАНАЛИ СИСТЕМ БЕЗПЕКИ.....	41
2.1 Аналіз особливостей природніх і штучних збурень, що можуть погіршити ефективність безпроводових систем безпеки.	41
2.2. Порівняння ефективності засобів захисту від зовнішніх збурень.	444
Висновки до розділу	52
3. ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ КОДУВННЯ ВІДЕОПОТОКУ В БЕЗПРОВОДОВИХ КАНАЛАХ СИСТЕМ БЕЗПЕКИ.....	53
3.1 Аналіз процесу відтворення потокового відео в реальному часі	53
3.2 Алгоритм відновлення відеоданих	56
3.3 Метод виявлення відеопідробки.....	60
3.4 Результати експерименту та їх аналіз	62
3.5 Якість відеозображення	63
3.6 Затримка зображення	65
3.7 Ефективність передавання.....	67
3.8 Безпека передавання	69
Висновок до розділу.....	70
4. РОЗРОБКА СТАРТАП-ПРОЄКТУ	73
4.1 Основна ідея стартап – проєкту.....	73
4.2 Аналіз ринку і конкурентів.	73
4.3 Визначення цільової аудиторії.	75
4.4 Опис мінімально життєздатного продукту.	76
Висновки до розділу	77
ВИСНОВКИ	79

СПИСОК ЛІТЕРАТУРИ	81
ДОДАТОК А	85

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ANT - протокол бездротової сенсорної мережі.

ARIB (Association of Radio Industries and Business) - Асоціація підприємств радіопромисловості та бізнесу.

CPSS (Cyber-Physical-Social system) - кібер-фізико-соціальної системи.

DVR (Digital Video Recorder) - Цифровий відеореєстратор.

GPRS (General Packet Radio Service) - Загальний сервіс пакетної радіопередачі.

GSM (Global System for Mobile Communications) - Глобальна система мобільного зв'язку.

HD (High Definition) - висока роздільна здатність.

IDEN (Integrated Digital Enhanced Networks) - Інтегрована цифрова розширена мережа.

IDR (Instantaneous Decoder Refresh) - Миттєве оновлення декодера.

IEEE (Institute of Electrical and Electronics Engineers) - інститут інженерів електротехніки та електроніки.

IFTTT (If This Then That) - Якщо це, то те.

IP - (Internet Protocol) - Інтернет протокол.

ISO (International Standardization Organization) - міжнародна організація стандартизації.

LLC (Logical link control) - управління логічним каналом.

MAC (media access control) - управління доступом до середовища.

NAL (Network Abstraction Layer) - Рівень абстракції мережі.

NALU (Network Abstraction Layer Units) - Одиниці мережевого рівня абстракції.

NVR (Network Video Recorder) - Мережевий відеореєстратор.

OSI (Open Systems Interconnection network model) - базова еталонна модель взаємодії відкритих систем.

PAN (Personal Area Network) - персональна мережа.

PDC (Personal Digital Cellular) - Персональний цифровий стільниковий.

RFID (Radio Frequency IDentification) - радіочастотна ідентифікація.

RTCP (RTP Control Protocol) - Протокол управління RTP.

RTMP (Real Time Messaging Protocol) - Протокол обміну повідомленнями в реальному часі.

RTP (Real-time Transport Protocol) - Транспортний протокол реального часу.

SDK (Software Development Kit) - комплект для розробки програмного забезпечення.

SIG (Special Interest Group) - групи спеціальних інтересів.

TCP (Transmission Control Protocol) - Протокол управління передачею.

UDP (User Datagram Protocol) - Протокол користувацьких датаграм.

UMTS (Universal Mobile Telecommunications System) - Універсальна система рухомого (мобільного) зв'язку

UWB (Ultra-Wide Band) - ультраширокий діапазон.

VCL (Visual Component Library) - Бібліотека візуальних компонентів.

WiMAX (Worldwide Interoperability for Microwave Access) - Всесвітня інтероперабельність для мікрохвильового доступу.

WLAN (Wireless Local Area Network) - безпроводова локальна мережа.

WMAN (Wireless Metropolitan Area Networks) - безпроводові мережі масштабу міста.

WPAN (Wireless personal area network) - безпроводова персональна мережа.

WWAN (Wireless Wide area network) - безпроводна глобальна обчислювальна мережа.

БСБ - безпроводові системи безпеки.

ВСТУП

На сьогоднішній день існує безліч систем безпеки для різних потреб людства. Це може бути що завгодно: від відеокамер у торгових центрах та на паркінгу, до високотехнологічних воєнних структур, де зберігають надважливу інформацію, зброю та вибухівку. Тобто, ці системи варіюються залежно від степені важливості та можливих ризиків. Іноді може вистачити декілька датчиків руху та звичайної системи сигналізації, а іноді потрібно броньована територія з металевим дротом по периметру, з попереджувальними знаками, прожекторами, охоронними турельними установками тощо. Як в першому так і у другому прикладі це можна класифікувати як системи безпеки.

Люди з давніх пір мріяли про безпроводові технології, так як частіше за все, прокладання кабелів створюють багато проблем. Вони об'ємні, плутаються між собою, в них є довжина, якої часто не вистачає, естетики в таких з'єднаннях теж небагато. Саме тому дослідження передачі інформації між пристроями через «повітря» була дуже актуальною проблемою. В сучасному світі наука вже знайшла вихід та на ринку у відкритому доступі можна купити собі смартфон, ноутбук, та багато інших безпроводових технологій. Такою ж є і технологія, яка є основною для аналізу в даній роботі.

Безпроводові системи безпеки – це наймолодші технології, які пропонують користувачеві. Вони мають свої плюси та мінуси, деякі з них очевидні, а деякі не такі передбачувані, як здається на перший погляд. В даній роботі проведено аналіз сучасних технологій БСБ та як вони працюють, аналіз ринку та можливі рішення, як в Україні так і в світі, технології передавання інформації, спосіб передачі та загальної роботи систем безпеки.

1. СТАН СУЧАСНИХ БЕЗПРОВОДОВИХ СИСТЕМ БЕЗПЕКИ

1.1 Аналіз особливостей сучасних безпроводових систем безпеки.

В даному розділі розглянемо певні види систем безпеки та класифікуємо їх по певних вибірках. Зазвичай більшість компаній та інформаційних джерел розділяють три види систем безпеки з точки зору бізнесу. До них належать:

- системи відеоспостереження та камери спостереження;
- системи контролю доступу;
- охоронні та тривожні сигналізації.

Кожен із цих видів являє собою великий розділ на підтипи охоронних систем. Першими розглянемо системи відеоспостереження та камери. Великі підприємства, які займаються як бізнес плануванням так і варіантами для охорони житлових будинків розділяють такі охоронні варіанти на наступні варіанти:

- системи відеоспостереження високої чіткості (HD);
- системи відеоспостереження на основі інтернет протоколу (IP);
- системи віддаленого моніторингу відеоспостереження.

Системи відеоспостереження високої чіткості забезпечують фантастичну якість зображення і дозволяють бачити все, що відбувається всередині і навколо території, яка потребує охорони.

Надійна та якісна система відеоспостереження високої чіткості забезпечує співробітникам, студентам, відвідувачам сайту, пацієнтам і клієнтам безпеку і душевний спокій.

Підприємства часто інвестують в системи відеоспостереження високої чіткості, щоб ловити і стримувати злочинців, захистити персонал, зменшити крадіжки на робочому місці та антисоціальну поведінку. Одним з брендів, які надають високоякісний захист цього типу, є компанія Hikvision.

Системи IP-відеоспостереження знайшли широке застосування з цілого ряду причин. На відміну від аналогових HD-систем, ці камери відеоспостереження інтегрують в існуючу інфраструктуру інтернет протоколу.

Наведемо декілька причин доцільності інвестування в такі системи:

- забезпечують поліпшену якість зображення в порівнянні з аналоговими системами відеоспостереження;
- можуть зекономити кошти за рахунок використання існуючої інфраструктури інформаційних технологій;
- охоплюють більшу площу, ніж аналогові камери відео спостереження;
- пропонують набагато більш потужні функції пошуку;
- мають чудові можливості розширення;
- допомагають ловити і стримувати зловмисників;
- перевіряють територію на предмет потенційних загроз безпеці.

Системи віддаленого моніторингу відеоспостереження користуються значним попитом серед великих компаній з обширною територією, яка потребує постійного захисту та спостереження завдяки ряду пропонованих переваг, пов'язаних з безпекою.

Завдяки віддаленому моніторингу систем відеоспостереження, камери безпеки контролюються 24/7 командою професіоналів в області безпеки.

Моніторинг відеоспостереження має багато переваг, в тому числі:

- зменшення впливу злочинності;
- стримування злочинців;
- заощадження коштів на охорону;
- виявлення більшої кількості загроз безпеці.

Однією з провідних компаній з напрямку моніторингу відеоспостереження є Arc Monitoring.

Наступний пункт – контроль доступу. Контроль доступу - це метод безпеки, спрямований на забезпечення доступу до, з і навколо бізнес-приміщень або ділянки. Наприклад, це може бути система на основі брелоків, що надає доступ до входних дверей для всього персоналу, але обмежує доступ до ІТ та серверних приміщень або система внутрішнього зв'язку - відео або аудіо, аналогова або ІР.

Контроль доступу охоплює багато областей, включно з:

- дверним системи входу;
- аудіодомофонами;
- відеодомофонами;
- ІР домофонами;
- картковими та брелоковими системами доступу.

Дверні системи входу виготовляють на основі потреб користувачів у забезпеченні безпечного доступу до території, що потребує певної охорони, з нею та навколо неї. Системи входних дверей містять таке апаратне забезпечення: відеодомофон і аудіодомофон, ІР-домофон, карткові та брелокові системи доступу.

Системи відеодомофонів пропонують додатковий рівень безпеки для суспільства при наданні людям доступу в будівлю або приміщення.

За допомогою відеодомофона можна побачити, хто знаходиться біля дверей, перш ніж впустити його. Як частина загальної системи контролю доступу, системи відеодомофонів - це спосіб:

- обмежити доступ до офісних приміщень;
- забезпечити безпеку і спокій – візуальна оцінка людини що запитує доступ;
- справляти враження на відвідувачів;
- керувати охороною здоров'я та безпекою.

Аудіодомофонні системи є ефективною формою контролю доступу для користувачів, які бажають убезпечити доступ до своєї будівлі, з неї та навколо неї.

Як і багато інших систем контролю доступу, аудіодомофони можуть бути інтегровані з іншими системами безпеки, такими як:

- системи відео спостереження;
- охоронна сигналізація;
- системи контролю доступу на об'єкті.

Спосіб реалізації цих систем безпеки може бути різним. Зазвичай вони охоплюють доступ до дверей та охоронні ситуації, зв'язок 1-2-1 і інтеграція з системами оповіщення.

ІР-домофонні системи набувають все більшої поширеності серед користувачів, які прагнуть забезпечити безпечний доступ до своєї будівлі, з неї та навколо неї.

ІР домофонні системи можуть використовувати як ззовні - на зовнішніх точках доступу, таких як ворота автостоянки, входні двері тощо, так і внутрішньо - для обмеження доступу в певні зони будівлі, такі як серверні, приміщення для зберігання дрібних грошей тощо. Як відео-, так і аудіодомофонні системи можуть легко працювати через ІР.

Незалежно від того, потрібен відеодомофон чи аудіодомофон, сучасні компанії рекомендують рішення на основі ІР-технологій. Існує величезний спектр переваг ІР-інтерком систем для бізнесу, а саме:

- гнучкість;
- безпека і спокій;
- швидка, проста установка;
- запобігання злочинам;
- захоплення даних (відвідувачів сайту);

- продуктивність та якість;
- масштабованість;
- імідж компанії.

Карткові та брелокові системи доступу. Системи доступу до дверей за допомогою брелоків, також відомі як системи безключового доступу, є надійним засобом контролю доступу до будівлі та приміщень користувача та виходу з них.

Системи доступу за допомогою брелоків допомагають звести до мінімуму ризику втрати ключів від офісних дверей та пов'язані з цим витрати на заміну дверних замків. Крім втрати, ключі можуть бути клоновані, що створює додаткові ризики для безпеки бізнесу.

Системи доступу за допомогою брелоків можуть бути запрограмовані, що дозволить знати, хто знаходиться в будівлі і де вони знаходяться.

Можна використовувати ці системи для моніторингу персоналу, такі як:

- відвідуваність;
- облік робочого часу;
- продуктивність.

Існують різні способи використання систем доступу до дверей за допомогою брелоків:

Зовнішні - на в'їзних воротах, вхідних дверях офісу або зовнішніх об'єктах, таких як сміттєві баки магазинів.

Внутрішні - для дозволу і обмеження доступу в певні зони і контролю за тим, хто де знаходиться в будівлі.

Останній пункт вибірки видів систем безпеки – це охоронні сигналізації. До них відносяться:

- проводові системи сигналізації;
- безпроводові системи сигналізації;
- системи сигналізації з моніторингом.

Безпроводові системи сигналізації досить поширені. На це є ряд причин:

- швидкість установки;
- неймовірна гнучкість у використанні;
- пропонують повну масштабованість.

Нові датчики можуть бути додані в нові місця, їх можна легко переміщувати, а відсутність необхідних кабелів забезпечує обмежені перебої в роботі і безперебійний процес установки.

Безпроводові сигналізації також сумісні з дистанційно контрольованою системою сигналізації, що забезпечує додаткову безпеку, швидке реагування і спокій.

На відміну від проводової сигналізації, безпроводова система охоронної сигналізації є повністю портативною. Це означає, що якщо користувач змінює місце розташування, систему можна переміщувати разом з ним.

Це може допомогти зменшити потребу в подальших експлуатаційних витратах, зберігаючи при цьому найвищий рівень безпеки. Якщо користувач планує розширювати свій охоронну зону або змінювати місце розташування, безпроводова охоронна сигналізація може бути розумним вибором.

Безпроводова система охоронної сигналізації має ряд основних переваг, основними з яких є:

- масштабованість - нові датчики можуть бути легко додані в мережу;
- повна сумісність з системами сигналізації з віддаленим моніторингом;

- плавний процес встановлення - обмежений збій у роботі вашого бізнесу;
- сумісність з іншими системами безпеки, такими як камери відеоспостереження;
- естетичність - немає необхідності в прокладанні великої кількості кабелів і магістралей навколо дверей і плінтусів;
- низькі витрати на встановлення в порівнянні з дротовими системами сигналізації.

Проводові системи сигналізації. Для споживачів, які потребують надійність і довговічність, проводова система охоронної сигналізації є майже єдиним правильним вибором.

Хоча безпроводові системи безпеки швидко оновлюються, вони можуть бути ненадійними і більш схильні до збоїв в роботі системи. Це необхідно враховувати при плануванні, якщо потрібно підвищити свою безпеку.

Проводові системи охоронної сигналізації пропонують таку ж функціональність і допомагають управляти тими ж загрозами безпеки, що і безпроводові системи.

Як і будь-яка інша охоронна сигналізація, проводову сигналізацію призначено для виявлення зловмисників і сповіщення про них завдяки звукового сигналу і повідомлення на смарт-пристрій.

Існує кілька ключових відмінностей, які слід враховувати при виборі між проводовою та безпроводовою системою. Однією з ключових переваг проводової сигналізації є те, що вона вимагає лише мінімальних поточних витрат.

На відміну від безпроводової сигналізації, немає необхідності в заміні батарейок. У разі зносу або обриву кабелю система сповіщає про несправність [20] .

Зазначимо переваги проводових систем сигналізації:

- повна сумісність з системами сигналізації з дистанційним моніторингом;
- низькі поточні експлуатаційні витрати - немає необхідності регулярно замінювати батареї;
- високий рівень безпеки та знижений ризик хибних тривог;
- сумісність з іншими системами безпеки, такими як камери відеоспостереження;
- естетичність - немає необхідності в прокладанні великої кількості кабелів і магістралей навколо дверей і плінтусів;
- низькі витрати на обладнання в порівнянні з безпроводовими системами сигналізації.

Системи охоронної сигналізації з моніторингом. Для споживачів, які потребують оптимального рівня безпеки в своїх приміщеннях і навколо них, система сигналізації з віддаленим моніторингом є доцільним вибором.

Зазвичай компанії самі контролюють і управляють своїми системами безпеки, і в багатьох випадках це дає їм необхідні гарантії надійності. Однак для підприємств, які потребують додаткової безпеки, слід розглянути можливість встановлення системи сигналізації з моніторингом.

Системи безпеки можуть бути налаштовані таким чином, щоб при спрацьовуванні сигналізації сповіщати поліцію. Чітко видимі знаки будуть діяти як стримуючий фактор - наявність поліції за спрацюванням-викликом допоможе зловити злочинців.

Моніторинг охоронної сигналізації - це зв'язок сигналізації з центральною станцією. У разі загрози безпеці, контрольна панель запускає подію і відправляє сигнал тривоги на центральну станцію моніторингу. Станція моніторингу сигналізації потім повідомить відповідні органи, в більшості випадків – це поліція.

Зазначимо переваги систем сигналізації з моніторингом:

- системи допомагають зменшити вплив злочинної діяльності навколо приміщень;
- влада повідомляється негайно, що скорочує час, необхідний злочинцям для здійснення своєї діяльності;
- швидке реагування – диспетчерська служба нічого не пропустить, на відміну від охоронців на місці, які можуть бути зайняті патрулюванням;
- надійність, при перебуванні поза приміщенням – нерухомість перебуває під ефективним моніторингом на предмет злочинної діяльності.

Також можна інтегрувати свої охоронні сигналізації з системами відеоспостереження, щоб допомогти затримати зловмисників на місці злочину.

Страхування – деякі страховики вимагають, щоб підприємства мали сигналізацію, щоб виправити поліс.

Віддаленість – особа, відповідальна за безпеку підприємства, може жити в годині їзди від офісу, складу або приміщення. Система сигналізації, що контролюється, забезпечує набагато швидший час реагування, допомагаючи зменшити вплив несанкціонованого проникнення, вторгнення тощо [20] .

Стандартні системи безпеки

Зазвичай, в базові комплекти охоронних систем безпеки входять безліч різних технологій, що забезпечують користувача не тільки безпекою з точки зору проникнення на територію, але й різні інші можливості для запобігання пожежі або протікання води. Так як дослідження стосується безпроводових систем, доцільно звернути увагу саме на технології цього напрямку безпеки.

До типових пристроїв, як елементів апаратного забезпечення систем безпеки належать:

- охоронні центральні для розумної безпеки (хаби);
- датчики протікання води;
- датчики руху;
- пожежні датчики;
- датчики відчинення;
- акустичні датчики розбиття скла;
- сирени;
- ретранслятори радіосигналу;
- пристрої керування [22] .

1.2. Порівняння застосовних безпроводових технологій в системах безпеки.

Для задіяння безпеки потрібно розглянути певну кількість інформації, яка стосується охорони інформації, що буде задіяна в системі. До такої інформації належать протоколи.

Усе різноманіття протоколів безпроводового передавання даних можна класифікувати кількома різними шляхами, обравши як основний один із параметрів, наприклад топологію мережі, швидкість роботи або алгоритми безпеки. Найпоширеніший метод класифікації в технічній літературі виходить із максимального радіуса дії безпроводової мережі. Нижче наведено класифікацію розглянутих протоколів за порядком зменшення радіуса [2] .

WWAN (Wireless Wide area network) - переважно це мережі стільникового зв'язку, їхній радіус дії становить десятки кілометрів. До цих мереж належать такі протоколи: GSM, CDMAone, iDEN, PDC, GPRS і UMTS.

WMAN (Wireless Metropolitan Area Networks) - це бездротові мережі масштабу міста. Радіус дії таких мереж кілька кілометрів. Прикладом протоколу цієї мережі слугує WiMAX.

Wireless LAN (Wireless Local Area Network; WLAN) - це бездротова локальна обчислювальна мережа. Радіус дії цього класу мереж - кілька сотень метрів. До них належать такі протоколи: UWB, ZigBee, Wi-Fi [5] .

WPAN застосовують для зв'язку різних пристроїв, включно з комп'ютерами, побутовими приладами та оргтехнікою, засобами зв'язку тощо. Радіус дії WPAN становить від кількох метрів до кількох десятків метрів. WPAN використовується як для об'єднання окремих пристроїв між собою, так і для зв'язку їх із мережами вищого рівня. Прикладом таких мереж можуть слугувати протоколи RuBee, X10, Insteon, Bluetooth, Z Wave, ANT, RFID.

Нижче стисло наведено кожен із зазначених протоколів. Ці протоколи обрано для аналізу внаслідок їхнього широкого поширення в сучасних безпроводових мережах зв'язку. Такий вибір дозволяє дати огляд поточного стану інформаційної безпеки в мережах безпроводового зв'язку незалежно від вирішуваних безпроводовими мережами завдань.

Модель OSI. Крім радіусу дії мереж роль протоколів важлива при визначенні рівнів у моделі OSI. Еталонна модель OSI, іноді звана стеком OSI, передбачає 7 – рівневу мережеву ієрархію, розроблену Міжнародною організацією зі стандартів (International Standardization Organization - ISO). Слід зазначити, що багато з розглянутих нижче протоколів було розроблено IEEE. Група протоколів IEEE 802.X містить опис мережевих специфікацій і дає стандарти, рекомендації та інформаційні документи для мереж і телекомунікацій. Рекомендації IEEE пов'язані головним чином із двома нижніми рівнями моделі OSI - фізичним і канальним. Ці рекомендації ділять канальний рівень на два підрівні: нижній - MAC (управління доступом до середовища) і верхній - LLC (управління логічним каналом) [9] .

Bluetooth. Протокол передавання інформації безпроводовим каналом зв'язку Bluetooth було розроблено групою компаній Ericsson, IBM, Intel, Toshiba і Nokia. Група розробки була створена на початку 1998 р. 20 травня 1998 р. відбулося офіційне представлення спеціальної робочої групи (SIG - Special Interest Group), покликаної забезпечити безперешкодне впровадження технології, що отримала назву Bluetooth. Bluetooth забезпечує обмін інформацією між такими пристроями, як кишенькові та звичайні персональні комп'ютери, мобільні телефони, ноутбуки, принтери, цифрові фотоапарати, мишки, клавіатури, джойстики, навушники, гарнітури на надійній, недорогій, повсюдно доступній радіочастоті для ближнього зв'язку. Зв'язок цих пристроїв може здійснюватися в радіусі від 10 до 100 метрів один від одного навіть у різних приміщеннях.

Протокол UWB розробив альянс компаній WiMedia, а 2007 р. цей протокол було затверджено як міжнародний стандарт ISO/IEC 26907. WiMedia UWB є стандартом широкосмугового безпроводового зв'язку на коротких відстанях. Протокол зачіпає аспекти взаємодії між пристроями на фізичному рівні (PHY) і підрівні доступу до середовища (MAC). Максимальна швидкість передавання даних між пристроями WiMedia UWB становить 480 Мбіт/с (як і в проводового USB), пристрої працюють у діапазоні частот від 3,1 ГГц до 10,6 ГГц. Протокол UWB конкурує з протоколом Bluetooth [3].

Протокол ZigBee - це стандарт для недорогих, малопотужних бездротових мереж із комірчастою топологією. Низька вартість дає змогу широко застосовувати цю технологію для безпроводового контролю та спостереження, а завдяки малій потужності сенсори мережі здатні працювати довгий час, використовуючи автономні джерела живлення. Протокол був розроблений альянсом компаній ZigBee. Цей альянс служить органом, що визначає для ZigBee стандарти високих рівнів; він також публікує профілі додатків, що дає змогу виробникам вихідних комплектуючих випускати сумісні продукти. Нижні рівні для цього стандарту розроблені IEEE і визначено стандартами IEEE 802.15.4-2006.

INSTEON розроблено для керування безпроводовими пристроями, призначеними для "розумного будинку". У протоколі передбачено зворотну сумісність зі старішим протоколом X10. Швидкість передавання сигналу керування за новим стандартом набагато вища, передбачено вбудовані засоби виявлення помилок і повторного передавання сигналу, а для передавання використовують гібридний канал - радіозв'язок і мережу електроживлення. Однак на відміну від X10 специфікації INSTEON захищені патентами і використовують тільки його розробниками - компанією Smarthome Technology [5].

Z-Wave з функціями самоорганізації та самовідновлення в поєднанні з гнучкими інсталяційними процедурами являє собою просте у використанні мережеве рішення. Протокол Z-Wave і чип високого ступеня інтеграції забезпечує невисоку вартість без компромісу щодо надійності або універсальності. Реалізується сумісність додатків і пристроїв Z-Wave, випущених різними виробниками. Z-Wave підтримує повний спектр пристроїв, включно з пристроями, що живляться від мережі змінного струму, від батарей, пристрої з фіксованим розташуванням і переміщувани пристрої, а також пристрої, що виконують роль мостів з іншими протоколами. У технології Z-Wave вузли поділяються на три типи: контролери (Controllers), виконавчі механізми, що маршрутизують (Routing Slaves), і виконавчі механізми (Slaves). У реальній мережі всі типи пристроїв можуть працювати в будь-якій комбінації [11].

ANT був розроблений компанією Dynastream Innovations. Цей протокол насамперед розрахований на компактні пристрої з автономним живленням (трансивери, що використовують цей протокол, вирізняються винятково малим струмом споживання) для передачі відносно коротких пакетів даних. Протокол передбачає організацію відкритих і приватних бездротових мереж, зокрема складного типу з динамічною конфігурацією. Він створений на основі технології PAN (Personal Area Network) і підтримує шари 1-4 стека OSI (Open Systems Interconnection network model). Типове застосування такого протоколу - бездротові датчики. Несуча частота за протоколом ANT - 2,4 ГГц, кількість частотних каналів при цьому дорівнює 125 (крок 1 МГц у діапазоні 2400. . . 2524 МГц). Швидкість передавання даних по радіоканалом (включно з протоколом) може становити до 1 Мбіт/с [13] .

RuBee (IEEE P1902.1) - протокол двостороннього безпроводового зв'язку в місцевій регіональній мережі з використанням довгохвильового діапазону (LW) і пакетів даних не більше 128 байт. Протокол RuBee подібний до протоколів серії IEEE 802, також відомих як Wi-Fi (IEEE

802.11), WPAN (IEEE 802.15.4) і Bluetooth (IEEE 802.15.1). RuBee networked, працює за принципом точка-точка і є розвитком стандартів RFID. RuBee передбачає роботу на низькочастотній носійній (131 кГц), даючи змогу використовувати вузли мережі з малим споживанням енергії.

RFID Radio Frequency IDentification. Радіочастотна ідентифікація з'явилася понад тридцять років тому. У 1973 р. Маріо Кардулло і його співавтори опублікували патент US 3713148, що описує перший пасивний транспондер RFID (радіомітку). Розвиток і широке впровадження радіочастотної ідентифікації довго стримувалося відсутністю стандартизації. Але в 90-х роках минулого століття Міжнародна Організація Стандартизації (ISO) прийняла низку стандартів у галузі RFID (серія стандартів ISO 18000-6).

X10 - це міжнародний відкритий індустрійний стандарт, застосовуваний для зв'язку електронних пристроїв у системах домашньої автоматизації. Стандарт X10 визначає методи та протокол передавання сигналів керування електронними модулями, до яких під'єднані побутові прилади, з використанням звичайної електропроводки або безпроводових каналів. Стандарт X10 розроблено 1975 року компанією Pico Electronics (Шотландія) для управління домашніми електроприладами. Вважається, що це перший стандарт для домашньої автоматизації [16] .

Wi-Fi створено 1991 р. NCR Corporation/AT&T (згодом - Lucent Technologies і Agere Systems) у Нідерландах. Wireless Fidelity - "бездротова точність" – торгова марка Wi-Fi Alliance для бездротових мереж на базі стандарту IEEE 802.11. Зазвичай схема Wi-Fi мережі містить щонайменше одну точку доступу (так званий режим infrastructure) і щонайменше одного клієнта. Також можливе підключення двох клієнтів у режимі точка-точка, коли точка доступу не використовується, а клієнти з'єднуються за допомогою мережевих адаптерів "безпосередньо". Точка доступу передає свій ідентифікатор мережі (SSID) за допомогою спеціальних сигнальних пакетів

на швидкості 0.1 Мбіт/с кожні 100 мс. Тому 0.1 Мбіт/с - це найменша швидкість передачі даних для Wi-Fi. Знаючи SSID-мережі, клієнт може з'ясувати, чи можливе підключення до цієї точки доступу. У разі потрапляння в зону дії двох точок доступу з ідентичними SSID приймач може вибирати між ними на підставі даних про рівень сигналу.

PDC (Personal Digital Cellular) - стандарт стільникового зв'язку покоління 2G. Розроблений асоціацією ARIB (Association of Radio Industries and Business) у квітні 2001 р. Використовується виключно на території Японії. Нині кількість абонентів стільникового зв'язку, що працюють на цьому стандарті, скоротилася до 10 мільйонів осіб. Притому, що в період максимальної поширеності цього стандарту кількість абонентів досягала 80 мільйонів осіб. PDC використовує частотні канали по 25 кГц із модуляцією $\pi/4$ -DQPSK із трьома часовими слотами, що забезпечують передавання зі швидкістю 11.2 кбіт/с або 6 тимчасовими слотами зі швидкістю передачі 5.6 кбіт/с. PDC використовує два діапазони частот - 800 МГц і 1,5 ГГц [4].

IDEN (Integrated Digital Enhanced Networks) - технологія для мереж транкінгового та стільникового зв'язку, розроблена компанією MOTOROLA в 1994 р. В основі технології iDEN архітектура GSM, під час передавання використовують частотні канали по 25 кГц, при цьому для передачі даних використана частина каналу шириною 20 кГц, решта призначена для захисту каналу. Протокол набув широкого поширення в усьому світі. Діапазон частот - 821-825 МГц [19] .

Стандарт CDMAOne розроблено 1995 р. як технологічний стандарт групи ANSI. CDMAOne заснований на використанні CDMA (множинного доступу з кодовим поділом). Система CDMA IS-95 фірми Qualcomm розрахована на роботу в діапазоні частот 800 МГц, виділеному для стільникових систем стандартів AMPS, N-AMPS і D-AMPS. (Стандарти TIA IS-19, IS-20; IS-54; IS-55, IS-56, IS-88, IS-89, IS-90, (S-553). Подальший розвиток технології CDMA відбувається в рамках технології CDMA2000.

При побудові системи мобільного зв'язку на основі технології CDMA2000 1X перша фаза забезпечує передачу даних зі швидкістю до 153 кбіт/с, що дає змогу надавати послуги голосового зв'язку, передачу коротких повідомлень, роботу з електронною поштою, Інтернетом, базами даних, передачу даних і нерухомих зображень.

WiMAX (Worldwide Interoperability for Microwave Access) - телекомунікаційна технологія, розроблена з метою надання універсального безпроводового зв'язку на великих відстанях для широкого спектра пристроїв (від робочих станцій і портативних комп'ютерів до мобільних телефонів). Заснована на стандарті IEEE 802.16, який також називають Wireless MAN. Назву "WiMAX" було запропоновано WiMAX Forum - організацією, заснованою у червні 2001 р. для просування і розвитку технології WiMAX. Форум описує WiMAX як "засновану на стандарті технологію, що надає високошвидкісний бездротовий доступ до мережі, альтернативний виділеним лініям і DSL" Максимальна швидкість - до 1 Гбіт/с.

GSM (від назви групи Groupe Special Mobile, пізніше перейменований у Global System for Mobile Communications) (рос. СПС-900) - глобальний цифровий стандарт для мобільного стільникового зв'язку з розподілом частотного каналу за принципом TDMA і середнім ступенем безпеки. Розроблено під егідою Європейського інституту стандартизації електрозв'язку (ETSI) наприкінці 1980-х років. Комерційне використання стандарту почалося в середині 1991 р., а до 1993 р. було організовано 36 мереж GSM у 22 країнах. На додаток до європейських держав стандарт GSM обрали багато країн Південної Африки, Близького і Далекого Сходу, а також Австралія. На початок 1994 р. кількість абонентів GSM досягла 1.3 мільйона. Термін GSM є скороченням від Global System for Mobile telecommunications – глобальна система мобільних телекомунікацій. GSM належить до мереж другого покоління (2 Generation), хоча на 2010 рік умовно перебуває у фазі 2,75G завдяки численним розширенням (1G - аналоговий стільниковий

зв'язок, 2G - цифровий стільниковий зв'язок, 3G - широкосмуговий цифровий стільниковий зв'язок, комутований багатоцільовими комп'ютерними мережами, включно з Інтернетом). Стільникові телефони випускаються для 4 діапазонів частот: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц [14].

GPRS (General Packet Radio Service - пакетний радіозв'язок загального користування) - надбудова над технологією мобільного зв'язку GSM, що здійснює пакетну передачу даних. GPRS дає змогу користувачеві мережі стільникового зв'язку здійснювати обмін даними з іншими пристроями в мережі GSM і з зовнішніми мережами, включно з Інтернетом. Передача даних розділяється за напрямками "вниз" (downlink, DL) - від мережі до абонента і "вгору" (uplink, UL) - від абонента до мережі. Мобільні термінали поділяються на класи за кількістю одночасно використовуваних таймслотів для передавання та приймання даних. За даними за червень 2006 р., телефони підтримують до 4-х таймслотів одночасно для прийому по лінії "вниз" (тобто можуть приймати 85 кбіт/с за кодовою схемою CS-4) і до 2-х - для передачі по лінії "вгору" (class 10 або 4+2).

UMTS (Universal Mobile Telecommunications System - Універсальна Мобільна Телекомунікаційна Система) – технологія Телекомунікаційна Система) - технологія стільникового зв'язку, розроблена Європейським Інститутом Стандартів Телекомунікацій (ETSI) для впровадження 3G в Європі. Як спосіб передавання даних через повітряний простір використовується технологія WCDMA, стандартизована відповідно до проєкту 3GPP як відповідь європейських учених і виробників на вимогу IMT-2000, опубліковану Міжнародним союзом електрозв'язку як набір мінімальних критеріїв для мережі стільникового зв'язку третього покоління. Згідно зі специфікаціями стандарту, UMTS використовує спектри частот: 1885-2025 МГц для передачі даних у режимі "від мобільного терміналу до базової станції" і 2110-2200 МГц для передачі даних у режимі "від станції до терміналу". У США через зайнятість спектра частот у діапазоні 1900 МГц

мережами GSM виділено діапазони 1710-1755 МГц і 2110-2155 МГц відповідно. Крім того, оператори деяких країн (наприклад, американський AT&T Mobility) додатково експлуатують смуги частот 850 і 1900 МГц. Уряд Фінляндії на законодавчому рівні підтримує розвиток мережі стандарту UMTS900, що покриває важкодоступні райони країни і використовує діапазон 900 МГц (у цьому проєкті беруть участь такі компанії, як Nokia і Elisa).[17]

Топології

Усі перелічені бездротові мережі працюють в одному або декількох варіантах топології. На рисунку 1.1 графічно наведено принцип роботи топологій різних видів.

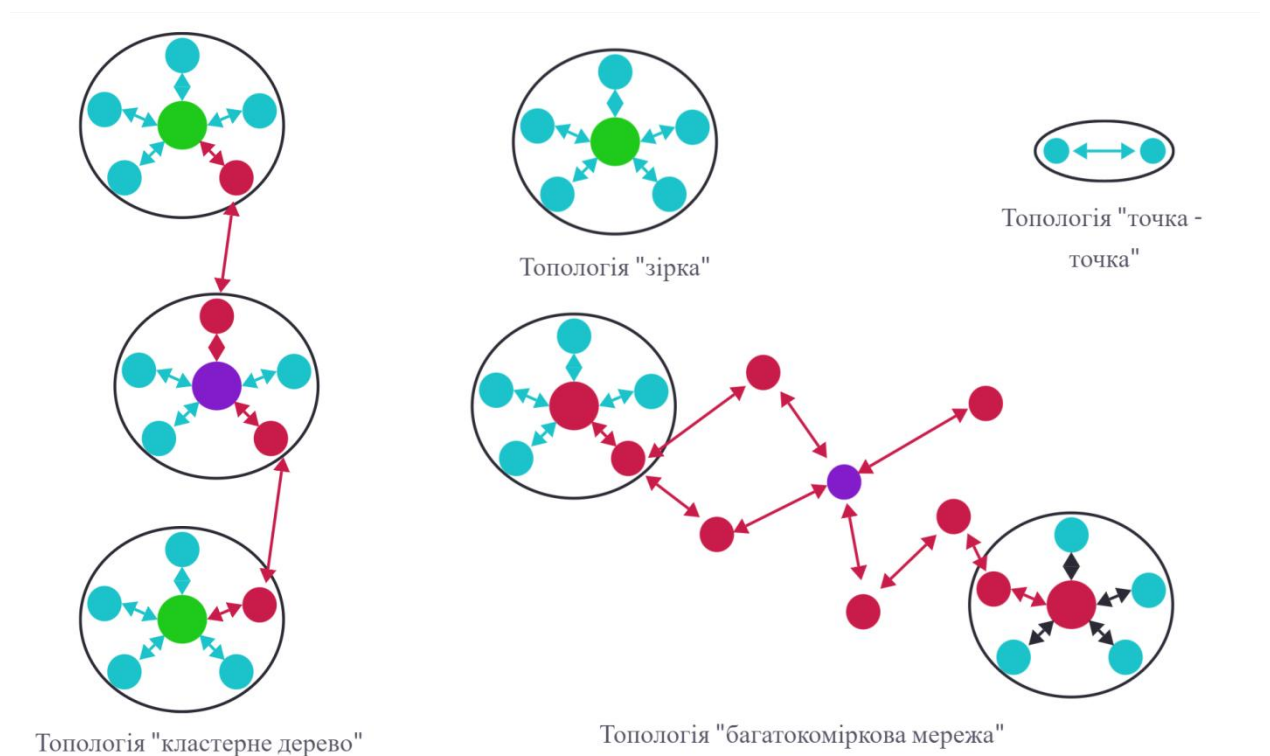


Рисунок 1.1 – Види топологій

Топологія "точка-точка" – найпростіший варіант організації мережі з двох пристроїв. Як правило, вузли цієї мережі є рівноправними, тобто мережа однорангова. Ця топологія характерна для Bluetooth, ANT, RFID, RuBee, PDC, WI-FI, Insteon, UWB, ZigBee та інших.

Топологія "Зірка" – служить основою організації всіх сучасних мереж зв'язку та обчислювальних мереж. Цю топологію використовують протоколи WI-FI, Insteon, ZigBee, UWB, IDEN, CDMAOne, WIMAX, GSM, GPRS, UTMS.

Топологія "багатокоміркова мережа" – базова повнозв'язкова топологія комп'ютерних мереж і мереж зв'язку, в якій кожна робоча станція мережі з'єднується з усіма іншими робочими станціями цієї ж мережі. Характеризується високою відмовостійкістю, складністю налаштування і надлишковою витратою кабелю в провідних мережах. Кожен вузол має кілька можливих шляхів з'єднання з іншими вузлами, за рахунок цього така топологія дуже стійка. Оскільки зникнення одного з каналів не призводить до втрати з'єднання між двома комп'ютерами. Ця топологія допускає з'єднання великої кількості вузлів і характерна, як правило, для великих мереж, її будують із повнозв'язної шляхом видалення деяких можливих зв'язків. Топологія застосовна для мереж із використанням протоколів UWB, WI-FI, Insteon, ZigBee, UWB, IDEN, CDMAOne, WIMAX, GSM, GPRS, UTMS.

Топологія "кластерне дерево" – утворюється в основному у вигляді комбінацій вищеназваних топологій обчислювальних мереж. Основа дерева обчислювальної мережі розташовується в точці (корінь), у якій збираються комунікаційні лінії інформації (гілки дерева). Обчислювальні мережі з деревоподібною структурою будують там, де неможливе безпосереднє застосування базових мережевих структур у чистому вигляді [3].

1.3 Стан апаратного забезпечення безпроводових систем безпеки

Апаратне забезпечення на ринку безпроводових систем безпеки є дуже різноманітним. Кожна компанія має свої рішення для охорони приватних територій і має велике різноманіття всіляких технологій для максимального комфорту та забезпечення клієнтів достатньою безпекою. На ринку існує багато компаній що надають охоронні послуги, які потрібно розглянути і порівняти, щоб мати цілісну картину з точки зору можливостей сучасних технологій та маркетингової складової. В даному підпункті розглянемо певну вибірку обладнання різних компаній.

Для аналізу була вибрана певна вибірка систем безпеки які є популярними у світі. Так як певної вибірки систем безпеки в Україні для аналізу знайти важко, із за домінуючої позиції компанії «Аджакс системс» на ринку. До вибірки увійшли такі пристрої, як: Wink (рис. 1. 3), Securifi Almond Guard, Nexia Home (рис. 1. 4), Piper та AJAX Hub 2 Plus (рис. 1. 5). Порівняння виконаємо за трьома загальними критеріями: загальне порівняння для користувача, наявність датчиків та аксесуарів системи та безпроводові протоколи передавання, що підтримуються.



Рисунок 1. 2 – Структура системи розумного будинку Wink

Зі структури системи розумного будинку Wink, зображеної на рис. 1. 2, можемо виділити обладнання, яке відповідає за контроль безпеки будівлі.

Безпроводова система безпеки Wink містить наступне обладнання:

1. Хаб Wink – відповідає за передавання сигналів від датчиків до власника, підтримує протоколи Bluetooth, Z-Wave (пристрій Z-Wave Plus з підтримкою захисту), ZigBee, Wi-Fi, Lutron Clear Connect, Kidde. Здатний підтримувати зв'язок за протоколом Z-Wave з такими типами пристроїв як дверний замок, датчик відчинення дверей/вікна, датчик руху, датчик нахилу, вимикач, регулятор освітленості, модуль приладів, і за протоколом ZigBee з лампочкою, вимикачем, розеткою, дверми/вікном.
2. Пожежна сигналізація Nest – розумний детектор диму та чадного газу, що здатний надсилати сповіщення на смартфон, якщо спрацює сигналізація та повідомляти про низький заряд, працює на шести батарейках типу AA.
3. Дверна ручка з клавіатурою Schlage з технологією Z-Wave. Миттєво відправляє сповіщення про відкриття дверей, має функцію віддаленого закриття або відкриття дверей, надсилає сповіщення про низький заряд батареї.
4. Розумний контролер гаражних воріт GoControl. Дозволяє відстежувати стан воріт на відстані, отримувати миттєві сповіщення про в'їзд і виїзд людей, а також керувати гаражем з будь-якого місця, з'єднується через Z-Wave з Хабом Wink. Радіус роботи – 30-50 футів (9-15 метрів).
5. Відеокамера DropCam Pro. Надсилає оповіщення, коли камера виявляє рух і звук, володіє нічним баченням, передає відеосигнал через Wi-Fi, що дозволяє переглядати зображення з камери віддалено.

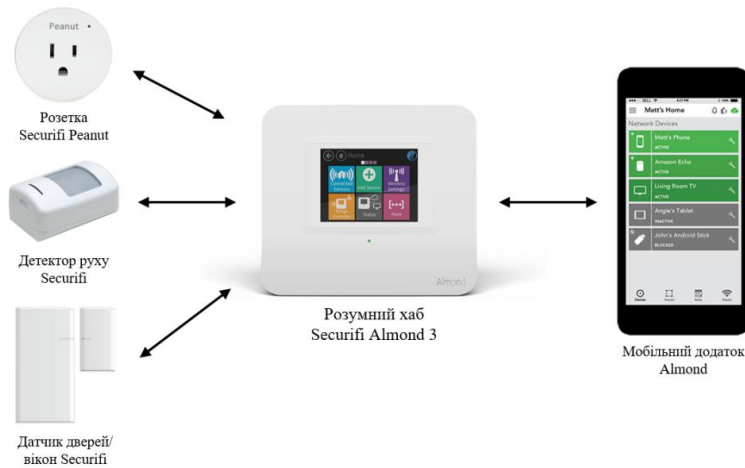


Рисунок 1.3 – Структура безпроводової системи безпеки Securifi Almond Guard

Зона покриття одного хабу Securifi Almond 3 складає 120 квадратних метрів. Різних будинків мають різні потреби сигналу Wi-Fi. Використання одного хабу підійде для невеликих квартир або одноповерхових будинків. Для середніх будинків необхідно використовувати два хаби, щоб покривати площу у 240 квадратних метрів, а для великих будинків знадобиться три хаби.

Almond Guard використовує декілька сигналів, таких як Wi-Fi, GPS, ZigBee та стільниковий зв'язок від пристроїв жителів будинку, щоб інтелектуально ставити та знімати будинок з-під охорони в потрібний час. Це також перша система домашньої безпеки, яка інтегрує кібербезпеку, захищаючи смарт-пристрої від хакерів і надаючи жителям будинку повну безпеку.

На ринку існують різні комплекти системи безпеки Securifi Almond Guard, розглянемо один з них, в яких входить наступне обладнання:

1. Хаб Securifi Almond 3S
2. Датчик дверей/вікон Securifi забезпечує віддалений контроль за станом дверей/вікон, надсилає повідомлення в разі зміни стану об'єкту моніторингу

3. Датчик руху Securifi – забезпечує віддалений контроль, надсилає повідомлення в разі фіксації руху.
4. Розетка Securifi Peanut – перемикач контролю живлення



Рисунок 1.4 – Структура безпроводової системи безпеки Nexia Home

Домашній інтелект Nexia використовує технологію Z-Wave, щоб надавати можливість комунікації приладів між собою та з власником.

Беспроводова система безпеки Nexia Home складається з наступних апаратних засобів:

1. Міст Nexia Home, як мозок системи, під'єднує всі компоненти Nexia до мережі інтернет.
2. Модуль диммера Schlage дозволяє власникам будинку контролювати їх світлове обладнання та малі побутові прилади віддалено.
3. Датчик руху Schlage та датчик дверей/вікон спроектований для відслідковування руху дверей та вікон, сенсори дозволяють власникам будинку віддалено визначати, коли двері або вікно відкрите або закрите.
4. Внутрішні та зовнішні камери Schlage для дому – сертифіковані Федеральною Комісією з комунікацій (FCC) безпроводові IP камери від фірми Schlage дозволяють власникам будинку записувати,

зберігати та переглядати відео їхнього будинку прямо зі смартфона або комп'ютера.

5. Сенсорний засув Schlage із вбудованим сигналом, входом без ключа та сумісністю з домашнім інтелектом Nexia.



Рис. 1. 5 – Структура безпроводової системи безпеки AJAX

Компоненти безпроводової системи безпеки AJAX:

1. Ajax Hub 2 Plus – централь системи безпеки, що має 4 канали зв'язку та працює у швидкісних мережах LTE. Така конфігурація дозволяє підключити пристрій до двох різних інтернет-провайдерів через Ethernet і Wi-Fi, а також до двох стільникових мереж. Водночас автоматичне перемикання між каналами займає секунди. Радіопротокол Jeweller забезпечує двосторонній зв'язок хаба з датчиками на відстані до 2000 м, дозволяє дистанційно керувати системою та повідомляє про тривогу менш ніж за 0,15 с.
2. Ajax MotionProtect – безпроводовий датчик руху, що повідомляє про перші ознаки вторгнення в дім або офіс. Кріпиться до стіни навпроти дверей та інших місць ймовірного проникнення злочинців.
3. Ajax DoorProtect – безпроводовий датчик відчинення, що повідомляє про перші ознаки вторгнення у приміщення внаслідок злому дверей

або вікна. Встановлюється на всі типи дверей, включно з металевою основою.

4. Ajax SpaceControl – кишеньковий брелок для керування режимами охорони. Має тривожну кнопку, щоб швидко сповістити близьких людей і охоронну компанію про загрозу.

Порівняємо зазначені системи за трьома загальними критеріями: загальне порівняння для користувача, наявність датчиків та аксесуарів системи та безпроводові протоколи передавання, що підтримуються.

В таблиці 1.1 наведено порівняння можливості та вартості систем безпеки для домівки. Порівняння виконувалось таким чином, щоб відповісти на запитання клієнта чи майбутнього користувача. Тобто, чи система встановлюється власноруч або компанією, порівняти їх за вартістю, як самого пристрою чи пристроїв, так і вартість установки, обслуговування, гарантійні терміни. Також важливою складовою є комплектація наборів за мінімальною вартістю, способи підключення, стільниковим зв'язком чи за допомогою Wi-Fi мережі.

Таблиця 1.1

Система	Wink	Securifi Almond Guard	Nexia Home	Piper	AJAX Hub 2 Plus
Моніторинг	Власноруч	Власноруч / професійна	Власноруч	Власноруч	Власноруч / професійна
Установка	Власноруч	Власноруч	Власноруч	Власноруч	Професійна
Вартість установки, грн.	0	0	0	0	250 - 500
Мінімальна вартість стартового набору, грн.	1 836,90 грн.	7347,60 грн.	2204,28 грн.	7347,60 грн.	8400 грн.

Продовження таблиці 1.1

Система	Wink	Securifi Almond Guard	Nexia Home	Piper	AJAX Hub 2 Plus
Складова набору	Тільки хаб	Тільки хаб	Тільки хаб	Камера + датчик руху + датчик проникнення	Датчик руху + датчик відчинення + брелок з тривожною кнопкою
Мінімальна вартість обслуговування, місяць	0 грн.	551,07 грн.	367,38 грн.	0 грн.	400 грн.
Максимальна вартість обслуговування, місяць	0 грн.	918,45 грн.	367,38 грн.	0 грн.	1000 грн.
Підключення	Wi-Fi	Wi-Fi, GSM	Wi-Fi	Wi-Fi	Ethernet, GSM, Wi-Fi
Повернення коштів (днів)	0	60	30	0	30
Гарантія (років)	0	3	0	0	2
Протоколи	Z-Wave + Zigbee	Proprietary	Z-Wave	Z-Wave	Jeweller

В таблиці 1.2 наведене порівняння пристроїв за наявними датчиками в системах безпеки. Вони не містять сторонні пристрої, такі як датчики протоколів Zigbee або Z-Wave.

Таблиця 1.2

Система	Wink	Securifi Almond+	Nexia Home	Piper	AJAX Hub 2 Plus
Камера	ні	ні	ні	так	ні
Карбоновий монітор	ні	ні	ні	ні	ні

Продовження таблиці 1.2

Система	Wink	Securifi Almond+	Nexia Home	Piper	AJAX Hub 2 Plus
Датчик вторгнення	так	так	так	так	так
Датчик розбиття скла	ні	ні	ні	ні	так
Датчик руху	так	так	так	так	так
Тривожна кнопка	ні	ні	ні	ні	так
Датчик присутності	ні	ні	ні	ні	ні
Дистанційне керування	ні	так	ні	ні	так
Сирена	ні	ні	так	ні	так
Датчик диму	ні	ні	ні	ні	так
Датчик температури	так	ні	ні	так	так
Терморегулятор	так	ні	ні	ні	ні
Датчик води	так	так	ні	так	так
Інше	Гараж			Вбудовані світло та аудіо	Ретранслятор, блок живлення

В таблиці 1.3 наведено системи безпеки, які мають той чи інший протокол. При виборі систем безпеки користувачі часто звертають увагу на єдину систему від одного виробника. Але, не кожна компанія надає весь спектр технологій для задовільнення потреб кожного користувача. Тому іноді потрібно комбінувати пристрої різних систем. Для цього потрібно враховувати сумісність пристроїв звертаючи увагу на протоколи взаємодії. Найпопулярнішими є – Z-Wave, Zigbee, Insteon і Wi-Fi, не зважаючи на унікальні рішення, такі як у компанії AJAX і їх Jewellery.

Таблиця 1.3

Система	Wink	Securifi Almond+	Nexia Home	Piper	AJAX Hub 2 Plus
Z - Wave	так	так	так	так	ні
Zigbee	так	так	ні	ні	ні
WiFi	так	так	так	ні	так
IFTTT	так	ні	ні	ні	ні
Jeweller	ні	ні	ні	ні	так

Висновки до розділу

Отже, існують безліч різних варіацій систем безпеки. Найперспективніші – безпроводові системи, так як вони є більш естетичними та зручними у використанні, хоча і мають свої недоліки які можна вирішити. Для коректної роботи безпроводові системи безпеки використовують різноманітні протоколи передачі інформації. Всі вони мають певні стандарти та зроблені так, щоб не перебивати сигнал і не створювати шум для інших елементів системи або навколишнього середовища. Найкращою компанією на ринку України з виготовлення безпроводових систем безпеки і однозначним лідером є компанія Ajax systems. Також, системи безпеки компанії є лідерами у різноманітності датчиків для системи безпеки та мають унікальний протокол передачі інформації, що погіршує шанс доповнити систему іншими пристроями сторонніх виробників але водночас робить її унікальною. Ціна на системи є нормальною, зважаючи на набори датчиків.

Для подальшого продовження дослідів потрібно визначити типи можливих завад, що можуть негативно вплинути на роботу безпроводових систем, так як частота, на якій працюють пристрої та інші фактори можуть негативно впливати на самі системи та призводити до погіршення їх роботи.

2. ВИЗНАЧЕННЯ ФАКТОРІВ ВПЛИВУ НА БЕЗПРОВОДОВІ КАНАЛИ СИСТЕМ БЕЗПЕКИ

2.1 Аналіз особливостей природніх і штучних збурень, що можуть погіршити ефективність безпроводових систем безпеки.

Безпроводові системи безпеки мають багато переваг та не меншу кількість недоліків. Одним з таких – завади та збурення, як природні так і штучні. До природних збурень можна віднести погодні умови які можуть вивести з ладу техніку, такі як шторм чи гроза. Також це електромагнітне поле Землі, що може створювати певні завади при передачі інформації на певних частотах.

До штучних завад може належати техніка власного дому, яка може заважати працювати одна одній, це може бути кімната з великою кількістю пристроїв, які працюють за протоколом Bluetooth. В таких умовах обладнання може не тільки заважати одне одному, а й заглушати частоти Wi-Fi мережі, що може дуже погано відобразитись на коректності роботи мережі. Також штучними збуреннями можна вважати дії зловмисників, які можуть спробувати вимкнути передавання сигналу за допомогою глушилок.

Розберемо варіант глушіння для завади роботи радіозв'язку та Wi-Fi мережі. Сам термін глушіння – це створення завад у радіоканалах, як правило, протизаконне. Використовується для затримки передачі тривоги у безпроводових системах безпеки. Сам процес глушіння виконується за допомогою пристроїв, так званих генераторів завад. Вони працюють у певному радіусі на тій же частоті що і у пристрою, який атакують. У випадку якщо частоти не збігаються, це ніяк не впливає на роботу пристрою.

Генератори завад бувають різних видів. Є пристрої які глушать певний, конкретний діапазон, а є широкосмугові, які глушать одразу кілька технологій зв'язку або цілі системи. Широкосмугові генератори завад відносять до трьох груп:

Портативні – пристрій невеликих габаритів з малою потужністю. Здатний працювати в діапазоні 5 – 15 метрів в ідеальних умовах.

Стаціонарні – дорожчий, потужніший та більший за розмірами варіант. Залежно від ціни та якості може мати більший діапазон та більшу можливість вразити декілька пристроїв. Принцип полягає в наступному, чим ширша смуга частот та діапазон дії, тим потужніший пристрій. Але така система із за великої потужності має недолік – вона сильно нагрівається, із через це потребує додаткового охолодження, відповідно, більших розмірів конструкції та ваги. Також чим більший діапазон частот тим більше антен, що також визначає габарити пристрою.

Саморобні – малопотужні пристрої що діють на дуже невеликі відстані, так як створення в домашніх умовах широкосмугового пристрою глушіння потребує спеціалізованих навичок та обладнання [23].

Далі необхідно розглянути, яким чином відбувається глушіння різних типів каналів. Канал GSM можна заглушити лише у випадку слабкості сигналу. Якщо сигнал є стабільним то заглушити такий вид передачі дуже важко, так як це означає, що потужність передавача стільникового оператора досить висока.

Проаналізуємо і патентні розробки фірми Ajax Systems, а конкретніше, частотний сигнал Jeweller. Технології на базі цього сигналу постійно вимірюють рівень шуму в радіоканалі на його частоті. Система безпеки реєструє глушіння на певному рівні потужності шуму, а саме, -70дБм протягом тридцяти секунд. При цьому хаб надсилає сповіщення про спробу глушіння і перемикається на іншу частоту, щоб продовжити безперервну роботу системи [23] .

Глушіння Wi-Fi систем відбувається на частотах 2,4 ГГц та 5 ГГц. Заглушити сигнал безпроводової передачі інтернету дуже легко, так як йому може перешкоджати і внутрішня система у домі, наприклад мікрохвильові печі та радіояншки, що працюють на частоті 2,4 ГГц. Тому, як правило, в

системах безпеки існують інші канали зв'язку, щоб запобігти невчасного переривання [3] .

Одночасне глушіння всіх трьох типів каналів - це дуже дорого та такий пристрій має великі габарити. Такий пристрій неможливо купити у вільному продажу. Якщо зловмисники і застосують такий потужний генератор завад, то патентовані системи, на кшталт тієї, що використовує компанія Ajax, відправляють інформацію про застосування нелегальних глушилок, хаб втрачить зв'язок із сервером і увімкне аварійну тривогу.

Як висновок можна зазначити декілька важливих пунктів:

- заглушити всі канали на професійних системах безпеки можуть лише дорогі та великогабаритні генератори завад;
- хороша та надійна система безпеки має мати хоча б два канали безпроводового зв'язку, та бажано мати підстраховку у вигляді проводового Ethernet кабелю;
- якщо зловмисникам зможуть заглушити систему, то про це все одно буде повідомлено як охоронну службу, так і користувача;
- у разі обірваного зв'язку з системою потрібно негайно перевірити охоронний пункт, в цей час група швидкого реагування буде відправлена на місце події [23] .

Щодо природніх збурень, то екстремальні температури є однією з головних причин відмови систем безпеки.

Холод - страшний ворог будь-якої системи безпеки, тому продукція створюється для роботи за температури до мінус 40 градусів за Цельсієм. Є два способи перевірити стійкість обладнання до холоду - або шляхом поступового зниження температури до -40 градусів, або запуску пристрою відразу за температури -40 градусів. Дослідження виявили, що важливо перевіряти роботу пристроїв в обох випадках, тому що більшість інтеграторів у холодних країнах встановлюють відеокамери одразу після того, як виймають їх з упаковки, у них немає можливості поступово знижувати

температурний вплив. Для функціонування на морозі система відеоспостереження потребує підтримання певної температури її компонентів. Високі значення на іншому кінці температурної шкали також можуть швидко призвести до проблем. Правильне рішення полягає в змозі не тільки зменшити багато проблем, пов'язаних із високою температурою, а й знизити потреби в технічному обслуговуванні та, відповідно, вартість.

Високі температури і вологість можуть швидко вивести систему з ладу, спричинивши проблеми з електронікою, рухомими частинами і конденсатом на елементах. Спекотні умови - велика проблема для електроніки тому в надзвичайних умовах рекомендується система яка витримує спеку до 65 градусів.

2.2. Порівняння ефективності засобів захисту від зовнішніх збурень.

Безпроводові системи безпеки зазвичай використовують декілька каналів зв'язку для повідомлення служб безпеки про те, що трапилось. Зазвичай це можуть бути GSM, Ethernet та Wi-Fi. Прості системи використовують тільки одну технологію, кращі ж виробники намагаються підключити хоча б дві з наведених, для того, щоб одна з систем передавання була завжди готовою попередити служби про небезпеку на території, що знаходиться під контролем. Ненадійність систем з одноканальним зв'язком можна пояснити тим, що використання GSM може перестати оповіщення із за не своєчасної оплати тарифу, в той час як Wi-Fi мережа буде працювати. Також, зловмисники можуть заглушити сигнал або обрізати провід Ethernet. Саме на такі випадки і розраховують компанії, додаючи багатоканальність у свої пристрої.

У багатоканальній системі повинен бути один основний та інші – резервні канали. Це слугує надійним варіантом, так як відмова кількох каналів одночасно є менш вірогідною і зберігає стабільну роботу в разі природнього або штучного втручання. Слід враховувати, чим більше каналів, ти більший шанс що система буде працювати без перебоїв. Також варто

враховувати що кілька однотипних модулів мають ті ж проблеми що і пристрої з одним модулем, тобто вони лишаються ненадійними і вважаються як одноканальні пристрої [24].

Провідні сучасні компанії в своїх хабах використовують гібридні системи, що містять усі три типи каналів зв'язку, тобто, Wi-Fi, Ethernet та 3G подвоєний слот під сім-картки, для максимально безпечної роботи двадцять чотири години на добу сім днів на тиждень.

Ще один із засобів захисту - це хмарний сервер. Він являє собою ланку яка сполучена з центральним сервером та програмним забезпеченням, що керує безпосередньо системою безпеки. За допомогою цієї технології можна контролювати аспекти роботи охоронної системи з будь-якої точки світу, як користувачем так і інженером, відповідальним за роботу при наявності інтернет зв'язку.

Якщо система професійна, то хмарний сервер також може контролювати валідність зв'язку з охоронним обладнанням і його стан, періодично відправляючи тестові запити, таким чином опитуючи централі. Варто звернути увагу на частоту запитів, чим вона вища, тим швидше сервер зможе виявити проблему і попередить як користувача, так і компанію про проблему.

У безпроводових системах безпеки обмін інформацією між централлю й датчиками здійснюють радіоканалом. Зв'язок має бути гранично надійним — навіть короточасні обриви небажані, бо вони призводять до збільшення часу передання тривоги, а втрата зв'язку взагалі неприпустима, бо централль, а слідом користувачі й охоронна компанія не дізнаються про тривожну подію.

Зазвичай професійні системи працюють на частотах 433 МГц або 868 МГц і використовують для зв'язку між централлю й датчиками діапазон частот, а не одну фіксовану частоту. Завдяки цьому система може

автоматично змінити робочу частоту в разі завад — випадкових чи навмисних. Технологія називається частотним гопінгом [24] .

Також потрібно додати, чому ж для зв'язку між пристроями не підходить Wi-Fi з'єднання. Це впливає з наступних причин:

- у багатоквартирних будинках і офісах частоти Wi-Fi (2,4 ГГц і 5 ГГц) дуже зашумлені і до того ж перевантажені пристроями: комп'ютерами, смартфонами, побутовою технікою. Це призводить до втрати даних під час передавання — «побутового глушіння»;
- якщо в передаванні даних через Wi-Fi задіяно мережеве обладнання об'єкта (роутери, маршрутизатори, репітери), стабільність їхньої роботи визначає працездатність системи безпеки;
- у Wi-Fi відносно невелика дальність зв'язку — приблизно 150 м за відсутності перешкод. Обмеження долається розгортанням багатокомпонентної мережі на об'єкті, але кожна нова ланка зменшує надійність системи безпеки [24] .

2.3 Сучасні програмні засоби моделювання впливу радіозавад на безпроводові системи безпеки.

В наш час при виготовленні БСБ використовують не лише апаратне забезпечення. Це також і програмне забезпечення для розрахунків можливих збоїв систем, впливів навколишнього середовища, симуляції різних катастроф тощо. Провідні кампанії в цій галузі допомагають виробникам оригінального обладнання та їх постачальникам у багатьох галузях промисловості вирішувати проблеми електромагнітної сумісності, пов'язані з проектуванням, аналізом і валідацією.

Для більш вузько направлених моделювань фізичних процесів є багато програм. Різниця такого програмного забезпечення в направленості, внутрішньому функціоналі та різноманітності інструментів зміни процесів.

Найвідоміші варіанти фізичного моделювання процесів – це MATLAB, Labview, Electronic Workbench. Розглянемо більш наочно кожен з цих програм.

MATLAB поєднує в собі середовище для персональних комп'ютерів, налаштоване для ітеративного аналізу і процесів проектування, з мовою програмування, яка безпосередньо виражає математику матриць і масивів. Він містить редактор Live Editor для створення сценаріїв, які поєднують код, вивід і форматований текст у виконуваному блокноті.

Можливості MATLAB:

- аналіз, моделювання та дослідження даних;
- візуалізація та дослідження даних;
- створення скриптів, функцій і класів;
- створення десктопних і веб-додатків;
- інтеграція зовнішніх мовних інтерфейсів, таких як Python, C/C++, Fortran, Java тощо;
- можливість виконувати великомасштабні обчислення;
- можливість передачі проєктів через Інтернет і локальну мережу;
- робота з хмарними середовищами, такими як інтегрованим MathWorks Cloud або AWS, Azure та іншими зовнішніми проєктами;
- розгортання в корпоративних додатках. Код MATLAB готовий до виробництва, тому можливо перейти безпосередньо до хмарних і корпоративних систем, а також інтегруватися з джерелами даних і бізнес-системами;
- запуск на вбудованих пристроях. Автоматично перетворюйте алгоритми MATLAB в код C/C++, HDL і CUDA для запуску на вбудованому процесорі або FPGA/ASIC;
- інтеграція з системами моделювання. MATLAB працює з Simulink для підтримки Model-Based Design, який використовується для

багатодоменого моделювання, автоматичної генерації коду, тестування і верифікації вбудованих систем [25].

Мова MATLAB є високорівневою інтерпретованою мовою програмування, що містить засновані на матрицях структури даних, широкий спектр функцій, інтегроване середовище розроблення, об'єктно-орієнтовані можливості та інтерфейси до програм, написаних іншими мовами програмування.

Програми, написані на MATLAB, бувають двох типів - функції та скрипти. Функції мають вхідні та вихідні аргументи, а також власний робочий простір для зберігання проміжних результатів обчислень і змінних. Скрипти ж використовують загальний робочий простір. Як скрипти, так і функції зберігаються у вигляді текстових файлів і компілюються в машинний код динамічно. Існує також можливість зберігати так звані pre-parsed програми - функції та скрипти, оброблені у вигляд, зручний для машинного виконання. У загальному випадку такі програми виконуються швидше звичайних, особливо якщо функція містить команди побудови графіків.

Основною особливістю мови MATLAB є її широкі можливості з роботи з матрицями, які творці мови висловили в гаслі "думай векторно" (англ. Think vectorized).

LabVIEW - це один з основних продуктів компанії National Instruments. Насамперед треба зазначити, що LabVIEW - це аббревіатура, яка розшифровується як Laboratory Virtual Instrumentation Engineering Workbench. Уже в назві простежується орієнтація на лабораторні дослідження, вимірювання та збір даних. Дійсно, побудувати SCADA-систему в LabVIEW дещо простіше, ніж при використанні "традиційних" засобів розробки. Це принципово інша мова програмування, або якщо хочете ціла "філософія" програмування. Функціональна мова, що змушує дещо інакше мислити і часом надає абсолютно фантастичні можливості для розробника. Сам по собі

LabView немає стандарту, як, наприклад ANSI C. Формально такої мови не існує, але в цьому і полягає принадність цього засобу розроблення: від версії до версії в мову вводяться все нові конструкції. Складно уявити, що в наступній реінкарнації Сі з'явиться, наприклад, нова структура для for-циклу. А в LabVIEW таке цілком можливо [26].

LabVIEW – це кросплатформне графічне середовище розроблення додатків, являє собою універсальну мову програмування. І хоча цей продукт часом тісно пов'язаний з апаратним забезпеченням National Instruments, він проте не пов'язаний з конкретною машиною. Існують версії для Windows, Linux, MacOS. Вихідні тексти переносяться, а програми матимуть однаковий вигляд у всіх системах. Код, згенерований LabVIEW, також може бути виконаний на Windows Mobile або PalmOS. Цю мову можна з успіхом використовувати для створення великих систем, для опрацювання текстів, зображень і роботи з базами даних.

LabVIEW - досить високорівнева мова. Однак ніщо не заважає включати "низькорівневі" модулі в LabVIEW-програми. Навіть якщо потрібно використовувати асемблерні вставки - це теж можливо, треба лише згенерувати DLL і вставити виклики в код. З іншого боку, високорівнева мова дає змогу запросто виконувати вельми нетривіальні операції з даними, на які у звичайній мові могло піти багато рядків (якщо не десятки рядків) коду. Втім, треба зазначити, що деякі операції низькорівневих мов (наприклад, роботу з покажчиками), не так просто реалізувати в LabVIEW, зважаючи на його "високорівневість". Мова LabVIEW містить основні конструкції керування, що мають аналоги і в "традиційних" мовах:

- змінні (локальні або глобальні);
- розгалуження (case structure);
- For - цикли з перевіркою завершення і без;
- While – цикли;

- групування операцій.

У LabVIEW розроблювані програмні модулі називають "Virtual Instruments" (Віртуальні Інструменти) або просто VI. Вони зберігаються у файлах із розширенням *.vi. У принципі кожен VI складено з двох частин - Блок-діаграма (Block Diagram) і Передня панель (Front Panel). Блок-діаграма - це програмний код (точніше візуальне графічне представлення коду), а Передня панель - це інтерфейс.

В основі LabVIEW лежить парадигма потоків даних. У програмному середовищі умовна константа і термінал індикатора з'єднані між собою лінією. Ця лінія називається Wire. Можна назвати її "дротом". По дротах передаються дані від одних елементів іншим. Уся ця концепція називається Data Flow. Суть Блок Діаграми - це вузли (ноди), виходи одних вузлів приєднані до входів інших вузлів. Вузол почне виконання тільки тоді, коли прибудуть усі необхідні для роботи дані. На діаграмі вгорі дві ноди. Одна з них - константа. Цей вузол самодостатній - він починає виконання негайно. Другий вузол - індикатор. Він відобразить дані, які передає константа (але не відразу, а щойно дані прибудуть від константи).

Всі елементи у програмі виконуються паралельно. В останніх версіях можна навіть явно вказати на якому з процесорів має виконуватися той чи інший while-цикл. Зараз існують надбудови і для текстових мов, що дають змогу запросто домогтися підтримки багатопроцесорних систем, однак так просто, як на LabVIEW, це, мабуть, ніде не реалізовано. Треба також зазначити, що в розпорядженні розробника багатий вибір інструментів для синхронізації потоків - семафори, черги, рандеву, тощо.

LabVIEW містить у собі багаті набори елементів для побудови користувацьких інтерфейсів. Стандартна поставка LabVIEW містить блоки для роботи з ini файлами, реєстром, функції для роботи з двійковими і тестовими файлами, математичні функції, потужні інструменти для побудови

графіків (а куди ж без цього в лабораторії), а на додачу до вже згаданої можливості викликів DLL, LabVIEW дає змогу працювати з ActiveX компонентами і .net. Починаючи з восьмої версії в LabVIEW було додано підтримку класів - мова стала об'єктно-орієнтованою. Реалізовану підтримку не можна назвати повною, проте основні риси об'єктно-орієнтованих мов - успадкування та поліморфізм - присутні. Також функціональність мови можна розширити додатковими модулями, як-от NI Vision Toolkit - для обробки зображень і машинного зору тощо. А за допомогою модуля Application Builder можна згенерувати виконуваний exe-файл. За допомогою Internet Toolkit можна працювати з ftp-серверами, за допомогою Database Connectivity Toolkit - з базами даних тощо.

Electronic Workbench – один із найвідоміших пакетів схематичного моделювання цифрових, аналогових і аналогово-цифрових електронних схем високої складності.

Дана система схемотехнічного моделювання показала досить високу гнучкість і точність обчислень, знайшовши широке застосування більш ніж у 50 країнах світу, як на підприємствах, так і у вищих навчальних закладах. Electronics Workbench включає інструменти для моделювання, редагування, аналізу та тестування електричних схем. Програма має простий інтерфейс і ідеально підходить для початкового навчання електроніки. Бібліотеки пропонують величезний набір моделей радіоелектронних пристроїв від найвідоміших іноземних виробників з широким діапазоном значень параметрів. Крім цього, є можливість створення власних компонентів. Активні елементи можуть бути показані як ідеальними, так і реальними моделями.

Різнманітні прилади (мультиметри, осцилографи, вольтметри, амперметри, частотні графопобудовники, динаміки, світлодіоди, лампи розжарювання, логічні аналізатори, сегментні індикатори) дають змогу робити вимірювання будь-яких величин, будувати графіки. Electronics

Workbench може провести аналіз ланцюга за постійним і змінним струмом, дослідити перехідні процеси за будь-якого зовнішнього впливу за допомогою генераторів сигналу різної форми. Для більш детального аналізу програмний пакет може працювати з PSpice і Micro-Cap. Electronics Workbench дає змогу експортувати результати робіт у трасувальники Tango, Orcad, Protel, Eagle і Layo1.

Висновки до розділу

Отже, при використанні безпроводових технологій, таких як системи безпеки також існують проблеми зі збуреннями, як штучними так і природніми. Щоб захистити систему від штучних збурень створено багатоканальні системи, що мінімізує ризик виводу з ладу системи. Від природніх же – спеціалізована техніка яка може витримати різноманітні тяжкі погодні умови, такі як спека або холод.

Для аналізу пристроїв та симуляцій збурень та роботи існує безліч програмного забезпечення. Кожне ПЗ є унікальним та підходить в окремих задачах. Найбільш функціональна з них – програма від компанії MATLAB, так як має широкий спектр для використання, має синергію з програмним забезпеченням SimuLink, що дозволяє не змінювати декілька варіантів середовищ і з'єднувати програмування з симуляцією в реальних умовах.

3. ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ КОДУВАННЯ ВІДЕОПОТОКУ В БЕЗПРОВОДОВИХ КАНАЛАХ СИСТЕМ БЕЗПЕКИ

3.1 Аналіз процесу відтворення потокового відео в реальному часі

У процесі відтворення відео в реальному часі двома найважливішими ланками є кодування відео та передача потокового відеосигналу. В даний час найбільш широко використовуваним стандартом стиснення відео є H.264/MPEG-4 AVC (H.264). Протокол передавання потокового мультимедіа зазвичай визначається як RTSP/RTP для задоволення більш високих вимог в режимі реального часу.

Заснований на традиційній гібридній структурі кодування з шаблоном прогнозування-трансформації, H.264 може підвищити ступінь стиснення за рахунок використання прогнозування кадру з декількома посиленнями, вектору руху з точністю 1/4 пікселя, цілочисельного перетворення та внутрішньопросторової оцінки, але має недолік - чутливість до помилок передачі. Біт помилки може спричинити серйозну деградацію якості декодування або навіть призвести до того, що відео не вдасться декодувати. Затримані пакети можуть бути відкинуті декодером через закінчення часу.

Кодування H.264 структурно поділяють на рівень кодування відео (VCL) та рівень мережевої абстракції (NAL). VCL несе кодовані дані, а NAL відповідає за упаковку і передавання даних. Відеофайл H.264 складено з набору блоків мережевого рівня абстракції (NALU), який містить обробку кодера та упаковані відеодані. Відповідно до типу фрагмента, включеного в NALU, існує три основні типи кадрів протоколу H.264: I-кадр, P-кадр та B-кадр. I-кадр, з повною інформацією для декодування, є незалежним і має великий обсяг даних, який може генерувати повну картину. P-кадр використовує одностороннє міжкадрове предиктивне кодування, яке потребує звернення до попереднього I-кадру або P-кадру для кодування і має менший обсяг даних. На P-кадр може вплинути помилка або відсутність опорного кадру, що може призвести до неможливості нормального

декодування. Кадр В приймає двонаправлене міжкадрове кодування передбачення, яке потребує переднього та заднього кадрів в якості опорного кадру. Кадр миттєвого оновлення декодера (IDR) є спеціальним І-кадром, тому що наступні Р-кадр та В-кадр не будуть використовувати будь-який кадр перед кадром IDR в якості опорного.

Кадр В не є важливим кадром під час передавання та відображення. Р-кадр також не є основним кадром, але, як правило, є незамінним. І-кадр та IDR-кадр є незамінними. Під час процесу передавання, незалежно від того, який тип кадру даних втрачено, це призведе до помилки процесу декодування, проявами якого є наступний кадр, пропуск кадру тощо.

RTP забезпечує наскрізні послуги передавання в режимі реального часу на основі протоколу датаграми користувача (UDP). Коли обсяг передавання даних великий, може відбуватися переупорядкування і втрата пакетів. Особливо, якщо роздільна здатність відео та частота кадрів високі або стан мережі поганий, фрагмент NALU з більшою ймовірністю може бути втрачений, що може призвести до неповного відтворення кадру відеоданих.

Наведемо аналіз особливостей цього процесу згідно [27]. Зокрема, при використанні RTP для передачі NALU-відеопотоку відправник інкапсулює кожен NALU в серію RTP-пакетів. Порядковий номер серії – $S_0, S_1, S_2, \dots, S_n$. Приймаюча сторона виконує відповідну обробку згідно з отриманим номером RTP-пакету. В ідеальному випадку відправник упакує відеопотік в серію RTP-пакетів з порядковими номерами $S_0, S_1, S_2, \dots, S_n$, а одержувач отримує повні пакети в порядку $S_0, S_1, S_2, \dots, S_n$. Припустимо, що приймаючий пакет має номер S_{ex} , а поточний отриманий пакет має номер S_{rep} :

$$S_{rep} = S_i (i = 0, 1, \dots, n); \quad (3.1)$$

На цьому етапі отриманий пакет є просто таким, який потрібно розпакувати, після чого пакет може бути проаналізований і безпосередньо

відображений. Однак, в реальних випадках, через складність і динамічність мережі, шляхи передачі пакетів і час прибуття на приймальний кінець не є однаковими. Як правило, існує багато ситуацій, в яких деякі останні пакети даних можуть прийти раніше, ніж попередні пакети. Тому проблема спотворення пакетів неминуча. Як це відбувається: приймач отримує пакет S_{rep} , а пакет, що підлягає розпакуванню S_{ex} , не є рівними. Якщо прийняті пакети не відсортовані, то при розборі відеоданих може виникнути помилка, і відео не зможе бути відтворено.

Як наслідок, на приймальній стороні повинен відбуватися процес повторного впорядкування пакетів. Для отриманого пакету, якщо $S_{rep} > S_{ex}$, він буде кешуватися і чекати на отримання наступного пакету. До тих пір, поки S_{rep} не стане рівним S_{ex} , то наступний пакет шукається в кеші від S_{ex} для розбору RTP пакета, і складання NALU для декодування і відображення. Якщо порядковий номер кешованого пакета не є безперервним, це означає, що RTP-пакет втрачено, процедура обробки буде пропущена, і всі RTP-пакети поточного NALU будуть відкинуті. Така обробка може викликати затримку відео та квітковий екран.

Крім того, розмір NALU відео високої чіткості, закодованого H.264, як правило, великий. Через обмеження максимальної одиниці передачі (MTU), RTP повинен прийняти спосіб упаковки відеоданих FU-A або FU-B (FU-A і FU-B, які є двома версіями одиниці фрагментації, ідентифіковані з номерами типу NALU 28 і 29 відповідно). Підхід FU-A або FU-B по суті розділяє NALU на кілька пакетів RTP, що збільшує ймовірність виходу з ладу або втрати пакетів під час процесу передачі та погіршує зниження якості відображення.

У порівнянні з ПК-середовищем, термінал мобільного пристрою слабший в обчисленнях, зберіганні та продуктивності мережі, вплив якості відтворення відео є більш очевидним. Тому він потребує спеціальної обробки для забезпечення ефекту відображення відео.

3.2 Алгоритм відновлення відеоданих

Проведемо огляд удосконалень, запропонованих в роботі [27]. Основна ідея запропонованого авторами алгоритму полягає в тому, щоб забезпечити змінний часовий діапазон для RTP-пакетів, які належать до однієї NALU. Всі проблеми, пов'язані з несправністю та втратою RTP-пакетів в межах NALU, будуть оброблятися в цьому часовому діапазоні. Якщо NALU є ключовим кадром, повторна передача втраченого RTP-пакету підтримується в межах змінного часового діапазону.

Коли програвач отримує RTP-пакети, для кешування RTP-пакетів використовується хеш-таблиця. У хеш-таблиці номер RTP-пакету та RTP-пакет утворюють пару ключ-значення. Коли програвач отримує RTP-пакет, його порядковий номер і вміст утворюють пару "ключ-значення" і їх вставляють в хеш-таблицю. На стороні програвача відповідний RTP-пакет постійно забирається з хеш-таблиці для відновлення NALU та декодування, як наведено на рисунку 3.1.

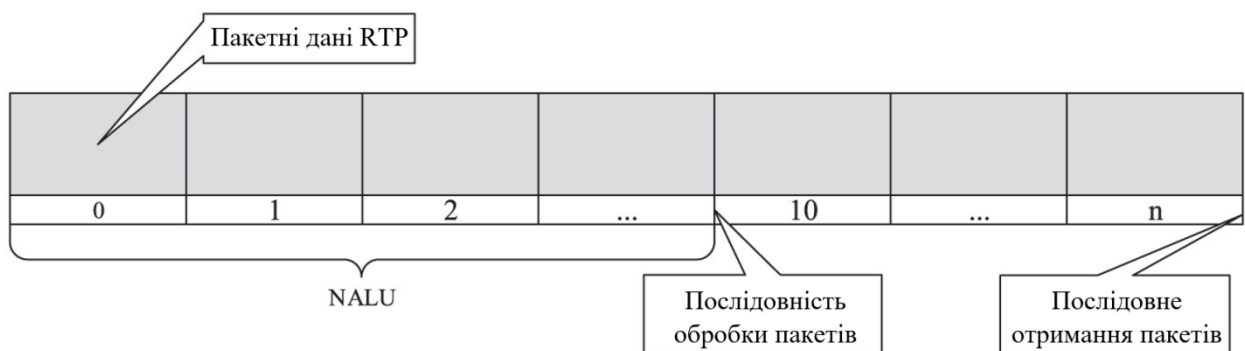


Рисунок 3. 1 – Використання хеш-таблиці для кешування RTP-пакету.

Як видно з рис.3.1, NALU може бути упакований в один або декілька RTP-пакетів. Таким чином, на приймальній стороні відображено кількість оброблюваних та прийнятих RTP-пакетів.

Під час передавання відеосигналу часові мітки RTP-пакетів, що належать до NALU, однакові, а порядковий номер RTP-пакету є безперервним. Тому при отриманні RTP-пакету, якщо мітка часу пакета

змінюється, це свідчить про те, що отримано RTP-пакет нового NALU. А раніше отримані RTP-пакети можуть складатися з повного NALU, який може бути безпосередньо наданий декодеру для декодування і відображення.

За умови, що номер і часова мітка поточного прийнятого RTP-пакета – це r і T_r , номер і часова мітка поточного декодованого RTP-пакета – це d і T_d . У процесі прийому при зміні часової мітки RTP-пакету може бути отримана множина P_{NALU} , що містить декодований RTP-пакет P_d до попереднього пакета $P_r - 1$ з поточного прийнятого. Елементи в наборі впорядковані. Конкретно це зазначено наступним чином:

$$P_{NALU} = \{P_d, P_d + 1, \dots, P_r - 1\} \quad (3.2)$$

Коли кількість елементів множини P_{NALU} дорівнює $r-d$, це свідчить про те, що пакети даних у множині є безперервними і NALU є повним, і може бути безпосередньо поданий на декодер для декодування.

Коли кількість елементів множини P_{NALU} не дорівнює значенню $r-d$, це означає, що не всі RTP-пакети NALU були отримані. NALU не може бути повністю сформована. Коли мітка часу пакета змінюється, це означає, що пакет RTP походить від нового пакета NALU. Отриманий RTP був використаний для сортування хеш-таблиці, так що, не розглядаючи випадок, коли пакет не в порядку, і коли мітка часу пакета змінюється, може бути два варіанти розвитку: один з них полягає в тому, що мітки часу RTP двох послідовних NALU змінилися, а інший – один або більше даних RTP між двома NALU можуть бути втрачені, тому мітки часу RTP двох переривчастих NALU змінилися, як наведено на рис. 3.2. Як видно з рисунка, пакети RTP з номером D та номером R належать до a NALU та $(n + a)$ NALU. Між двома NALU може бути $N(N \geq 0)$ NALU, тому такого роду розриви можуть виникати на одному елементі P_n або декількох елементах $P_n, P_n + 1, \dots (n = d, d+1, \dots, r-1)$.

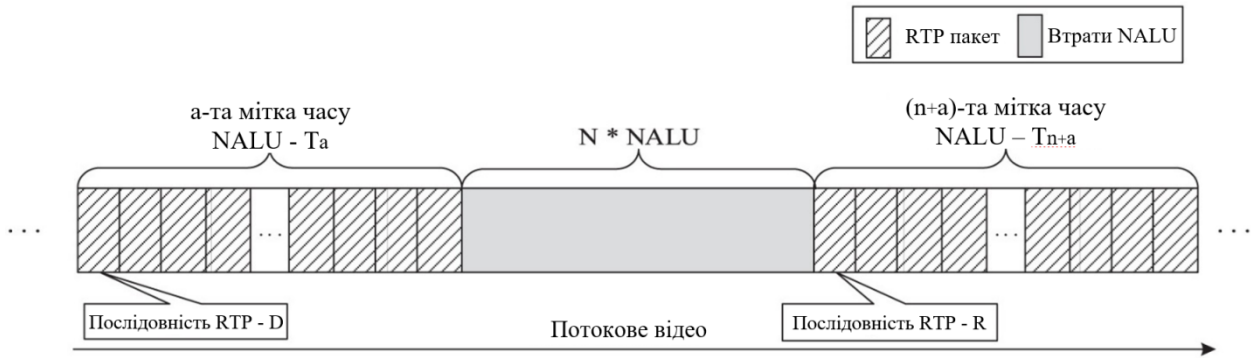


Рисунок 3.2 – RTP передача H.264 NALU.

Коли елементи в наборі P_{NALU} з'являються переривчастими, якщо NALU безпосередньо надсилається на декодер, якість зображення буде мати проблеми. Для того, щоб забезпечити функцію реального часу та певною мірою покращити якість зображення, ми використовуємо ковзне вікно для боротьби з неповною обробкою NALU.

Ковзне вікно призначене для досягнення мети корекції замовлення шляхом очікування пакета з невеликим серійним номером, який надійшов із запізненням. Ковзне вікно має дві часові межі: ліву межу W_l і праву межу W_r . Основними факторами, що впливають на розмір ковзного вікна, є середня кількість I-кадрів, упакованих в RTP-пакети, параметри відеосигналу і пропускна здатність каналу.

W_l можна обчислити за допомогою наступної функції. Розмір ковзного вікна хоча б трохи більше, ніж Num, щоб всі RTP-пакети I-кадру після виходу з ладу могли бути максимально досягнуті

$$W_l = \text{Num} + \frac{\text{Num} \times \text{MTU}}{S} \times (\text{fps} \times \text{Num}) \quad (3.3)$$

де Num - фіксована величина, яка представляє Num RTP пакетів, MTU - максимальна одиниця передачі (1500 байт), S - кількість байт відео, що приймаються програмою відображення в секунду, а fps – швидкість передавання кадрів відео.

W_r можна обчислити за допомогою наступної функції:

$$W_r = \lambda \cdot f \cdot \text{Num} + W_l \quad (3.4)$$

де $f \cdot \text{Num}$ - в ідеальному випадку кількість пакетів, що приймаються програвачем за 1 секунду, а λ є конфігураційним параметром програми і вказує на максимальний коефіцієнт коригування часу затримки програвача.

Зв'язок між значенням різниці кількості неотриманих і прийнятих пакетів W та межею вікна W_r і W_l визначається наступним чином:

1. Коли $0 < W < W_l$, це свідчить про те, що різниця в часі між неотриманим пакетом і прийнятим пакетом невелика, тому процес декодування може продовжувати чекати.

2. Коли $W_l < W < W_r$, NALU повторно організований всіма RTP-пакетами в наборі і готовий до декодування. Для RTP-пакету неключового кадру найпростішим методом є відкидання всіх даних набору та відкидання всіх RTP-пакетів неключового кадру, доки не буде отримано RTP-пакет ключового кадру, після чого розпочинається процес. Якщо RTP-пакет у наборі належить деякому ключовому кадру, він потребує обробки повторної передачі. Для пакету повторної передачі повинен бути механізм таймауту, механізм овертайму також може відповідати кількості пакетів, які змінюють значення W_l і нехай $W_l = W_l + \text{Num}$, після чого переходять на наступний прийом.

3. При $W > W_r$, пакет RTP у всьому наборі повинен бути відкинутий і перероблений з поточного пакету прийому P_r .

Представлений метод може бути використаний на етапі, що потребує отримання відеоданих з мережевого відеореєстратора або цифрового відеореєстратора (NVR/DVR), формування пакетів і передачу, а також організацію пакетів і відображення. Запропонований метод не потребує доопрацювання чи оновлення виробниками NVR/DVR, він дуже простий в експлуатації.

3.3 Метод виявлення відеопідробки

Через недостатній рівень захищеності існуючих технологій відеоспостереження зловмисники можуть використовувати такі методи для досягнення цілей атаки:

1. Зловмисник може імплантувати вірус, троянського коня або інший шкідливий код в комп'ютер або інші пристрої, щоб змусити термінал моніторингу продовжувати відтворювати фальшиве відео.

2. Зловмисник може передавати псевдомоніторингове відео не в режимі реального часу на термінал моніторингу за допомогою певного методу атаки з місця між камерою і терміналом моніторингу.

Всі ці методи атаки вводять в оману персонал, так що реальну ситуацію на об'єкті моніторингу неможливо отримати.

Проблему захисту відео при передаванні можна розглядати як проблему достовірної відмінності підроблених відеозаписів від непідроблених оригінальних. Схема підробки відеосигналу наведено на рис. 3.3 [27]. За умови, що відбувається вставка кадру, кадр m - кадр n - підроблена частина, кадр m і кадр b - з'єднання. Незалежно від того, яким є метод міжкадрової підробки, кадри навколо з'єднання повинні бути однаковими без будь-яких слідів, що залишаються на відео. Це означає, що кадр- a і кадр- m повинні бути однаковими, так само як і кадр- n і кадр- b .

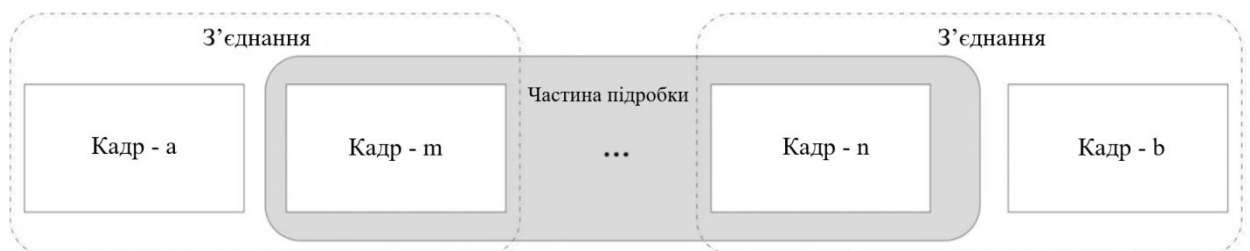


Рисунок 3.3– Схема відеопідробки.

В даному випадку для вирішення цієї проблеми пропонується метод виявлення відеопідробки на основі прив'язаного до часу токenu. Основна ідея

полягає в тому, щоб додати поле між заголовком RTP-паketу та відеоданими для представлення маркера. Один маркер повинен бути пов'язаний з часом, не може бути обчислений з попереднього маркера і може бути перевірений на іншій стороні. Крім того, значення маркерів в RTP-пакетах одного кадру (P/I-кадр) однакові, а значення маркерів RTP-пакетів в різних кадрах відрізняються. При передаванні відео в реальному часі як відправник, так і одержувач можуть обчислювати маркер кожного кадру окремо. Таким чином, при отриманні RTP-пакетів одержувач може перевірити відповідність токена в отриманих пакетах з власним розрахованим токеном, а потім виявити вставлене підроблене відео при виникненні атаки.

Ключовим моментом в даному методі є спосіб генерації токenu. Пропонований авторами [27] алгоритм, що відповідає поставленій вимозі, як наведено на рис.3.4. Генерація токenu повинна бути пов'язана з часом початку відтворення, щоб гарантувати, що вона пов'язана з процесом відтворення відео. Для процесу відтворення відео в реальному часі послідовність генерації токенів повинна бути однаковою у відправника та отримувача відео. Тобто, маркер, згенерований відправником, повинен відповідати маркеру, згенерованому одержувачем. Для вирішення цієї проблеми необхідно розробити функцію генерації послідовностей випадкових чисел на основі сіду (seed – зерно), і зробити так, щоб один і той же сід генерував одну й ту ж послідовність випадкових чисел. Таким чином, ми можемо забезпечити однаковий сід для відправника і одержувача під час однієї передачі, щоб вони могли згенерувати один і той же токен відповідну кількість разів. У цьому методі потрібно звернути увагу на обробку та перевірку маркера при втраті пакетів та повторній передачі I-кадру.

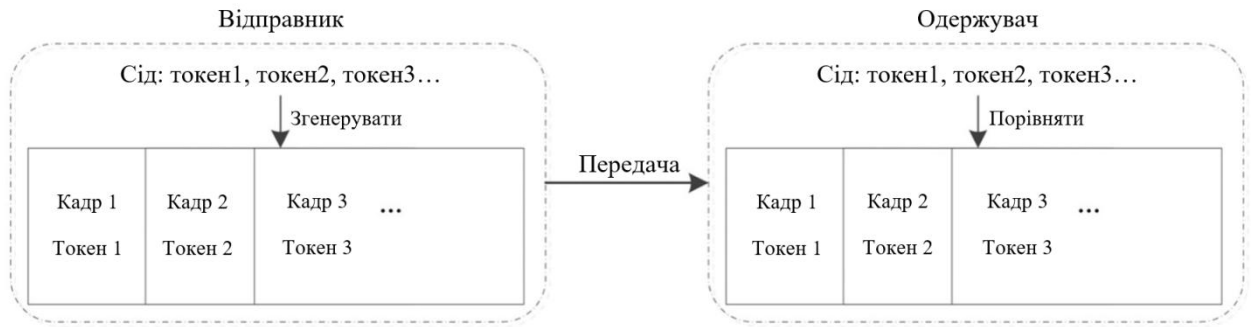


Рисунок 3.4 – Схема генерації послідовності токенів.

3.4 Результати експерименту та їх аналіз

У експерименті, проведеному дослідниками [27] використано камеру DS-2CD4232FWD-I (HIKVISION), три види відеопотоку в реальному часі використовувалися для вибірки даних. Кодування інформації становить (а) 15 кадрів в секунду, 720×480 ; (б) 15 кадрів в секунду, 1280×720 ; (в) 15 кадрів в секунду, 1920×1080 , відповідно, вибираючи 8-хвилинний відеопотік а, б і як відправника джерела вхідного відеосигналу.

Експеримент проведено у внутрішній мережі, ПК-відправник та мобільний телефон з програвачем знаходились в різних внутрішніх мережах. ПК-відправник використовував проводове з'єднання, а мобільний телефон використовував безпроводове з'єднання. Мережеве передавання між двома підмережами у внутрішній мережі не коливається протягом певного періоду часу. Всі експерименти, наведені нижче, виконано за безперервний проміжок часу.

Метою аналізованого алгоритму є поліпшення якості відеозображення в реальному часі та забезпечення безпеки відео в реальному часі в мережевому середовищі з поганими умовами передавання, При цьому немає значного впливу на продуктивність відео в реальному часі. Для того, щоб показати переваги алгоритму в основному порівнювали два звичайних сценарії передавання за цим алгоритмом. Тестові сценарії було обрано такі:

1. Стандартні сценарії передачі RTP/RTCP на основі UDP. Це передавання використовують в OpalVOIP, sipdroid та IMSDroid. Під час

обробки прийомання RTP, NALU, який втратив RTP-пакети, буде відкинуто, що дозволить уникнути помилки, спричиненої неправильним NALU, отриманим декодером. У цьому експерименті використано sipdroid як контрастний зразок.

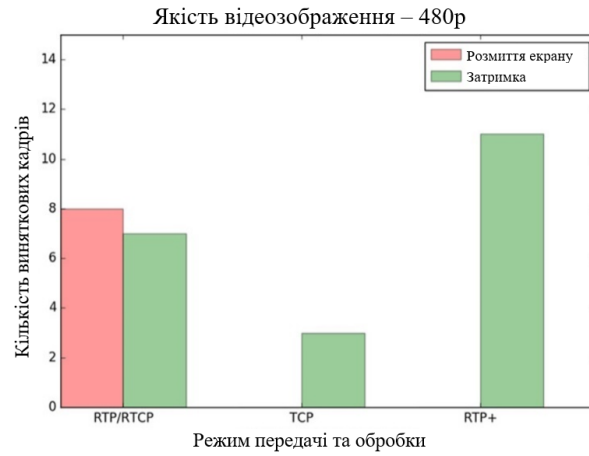
2. Передавання NALU на основі TCP. Тут об'єкт порівняння в основному віднесено до протоколу RTMP на основі TCP. Програмне забезпечення, що використовує протокол RTMP, часто є деякими SDK, що надано виробниками камер, такими як HCNetSDK від HIKVISION, та деякими вихідними програмними продуктами, такими як FFmpeg, ijkplayer. Тут використовується ijkplayer як зразок контрастності.

3. Вдосконаленому методу для протоколу RTP надано назва RTP+.

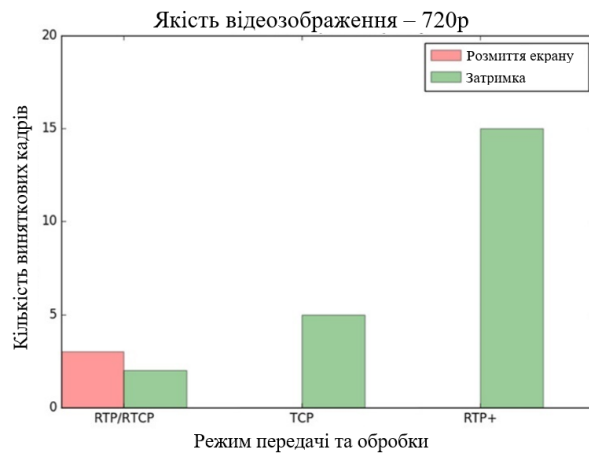
В експерименті проаналізовано алгоритм та інші методи з чотирьох аспектів: якість відеозображення, затримка зображення, ефективність передачі та безпека передачі.

3.5 Якість відеозображення

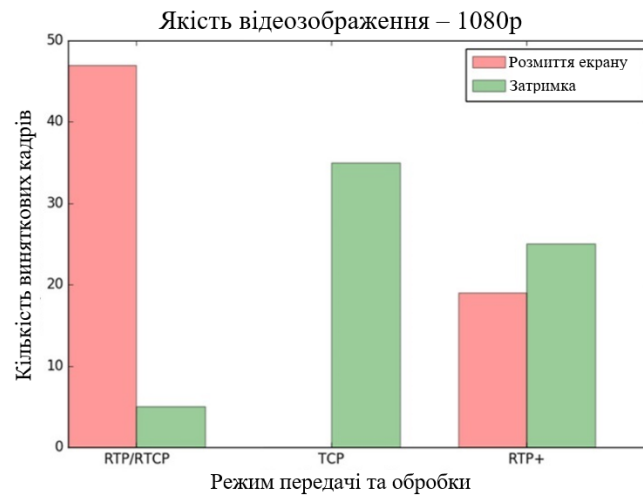
В одному і тому ж мережевому середовищі три типи відеопотоку (а, б і в) відображено у трьох вищезгаданих сценаріях. Зафіксовано кількість поточних та переривчастих кадрів, а для порівняння результати наведено на рис. 3.5. Як наведено на рис. 3.5, горизонтальна вісь є ознакою режиму передавання та обробки, а вертикальна вісь надає кількість разів аномального відображення відео. Кількість цих аномальних відображень підраховано за 8-хв. час відтворення.



а



б



в

Рисунок 3.5 - Порівняння показників зображення різної якості: а – 480p, б – 720p, в – 1080p.

За результатами, наведеними на рисунку 3.5, можна побачити, що зі збільшенням роздільної здатності відео та розміру даних запропонований алгоритм демонструє домінуючий приріст. При відтворенні відео з роздільною здатністю 720p протікань на екрані дисплея сцени 3 значно менше, ніж при використанні передачі сцени 1, але для сцени 2 особливих переваг не спостерігається. А при відтворенні 1080p перевага якості зображення методу очевидна. Тут менше відставання відео, ніж у сцені 2, і менше протікання кадрів, ніж у сцені 1.

Алгоритм відкидає неповний NALU не-I кадру та повторно передає неповний I кадр, що може зменшити кількість кадрів, що протікають та час відставання відео. Відкидання не-I кадру може спричинити пропуск кадру, але це не вплине на загальний ефект відображення під час фактичного процесу моніторингу.

3.6 Затримка зображення

Для того, щоб кількісно оцінити величину затримки зображення на екрані Δt , слід спочатку усунути різницю в часі між відправником і одержувачем. Δt можна розрахувати, виходячи з часу передавання T_s першого пакета і часу прийому T_r :

$$\Delta t = |T_s - T_r|. \quad (3.5)$$

При записі часу передачі і часу прийому в плеєрі в кінці деякого I-кадру, за допомогою Δt вносять поправку на різницю між цими двома значеннями часу, яка і є кількісно вимірюваним значенням уповільнення зображення.

Використано відео з роздільною здатністю 1080p, 15 кадрів за секунду формату H.264 які джерело вхідного сигналу і визначено ефект відтворення між різними методами. Для кожної сцени вибрано час відправки та час надання декодеру тридцяти I-кадрів. Після використання поправки Δt різниця

між цими двома часовими сегментами визначила затримку за різних методів. Результати наведені на рис. 3.6.

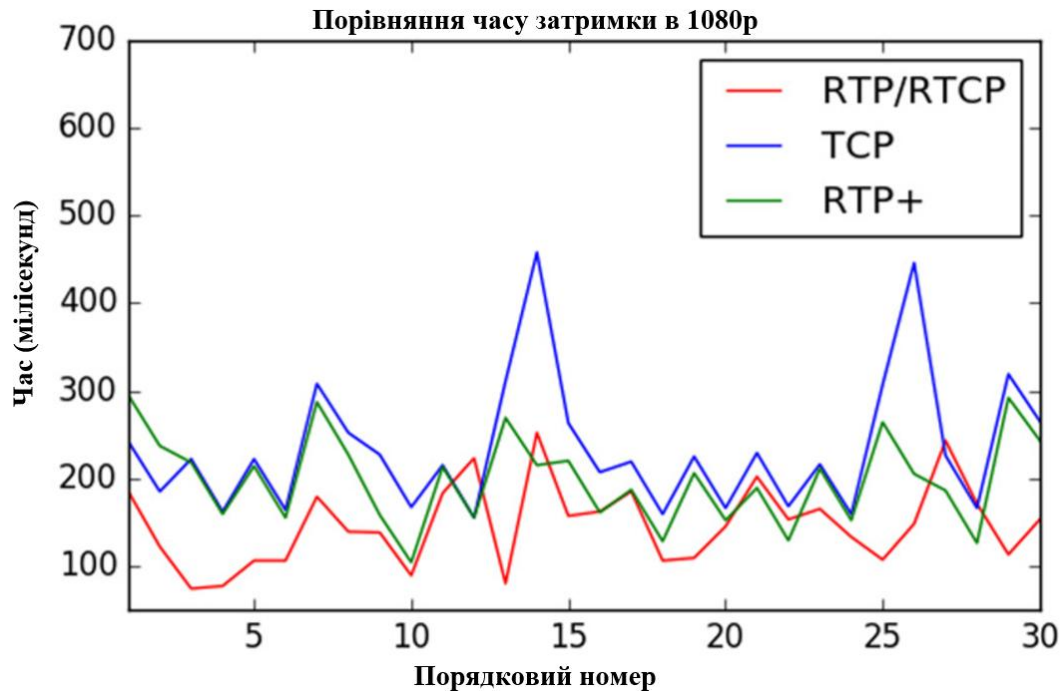
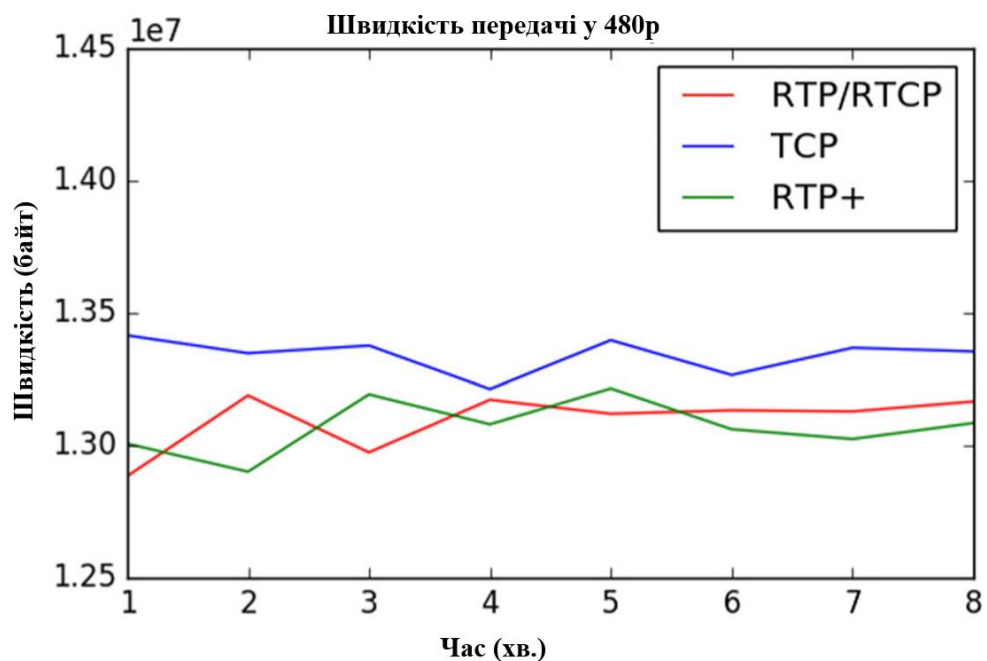


Рисунок 3.6 – Порівняння часу затримки.

Як видно з рис. 3.6, затримка сценарію 2 значно більша, ніж затримка сценарію 1 та сценарію 3, і навіть деякі NALU збільшилися в кілька разів. Затримка обробки NALU в сценарії 1 є мінімальною. У сценарії 3 затримка обробки NALU є відносно стабільною, але дещо більшою, ніж у сценарії 1. Цей результат також можна передбачити шляхом аналізу, коли передача даних є важкою, втрата пакетів буде відбуватися через перевантаження. Підхід протоколу TCP полягає в досягненні ретрансляції та підтвердженні, а стандарт RTP/RTCP заснований на протоколі UDP, який не має механізму, що гарантує надійність даних. За цим алгоритмом повторно передано ключовий кадр на основі роботи з порушенням порядку. Цей механізм ретрансляції має обмежену в часі ефективність, що не гарантує того, що втрачені дані можуть бути обов'язково повторно передані. Виходячи з аналізу отриманих результатів, запропонований алгоритм має очевидні переваги при високій роздільній здатності та якості відеосигналу.

3.7 Ефективність передавання

Використовуючи отримані дані з боку програвача, порівняно ефективність передавання відео в сценарії 1, сценарії 2 та сценарії 3. Результати наведено на рис. 3.7. Горизонтальна вісь на рисунку є показник часу, а вертикальна вісь - кількості переданих даних. Коли джерело відеосигналу має роздільну здатність 480р, швидкість передавання трьох сцен схожа, але при збільшенні роздільної здатності відео досліджуваний алгоритм показав певну перевагу.



а

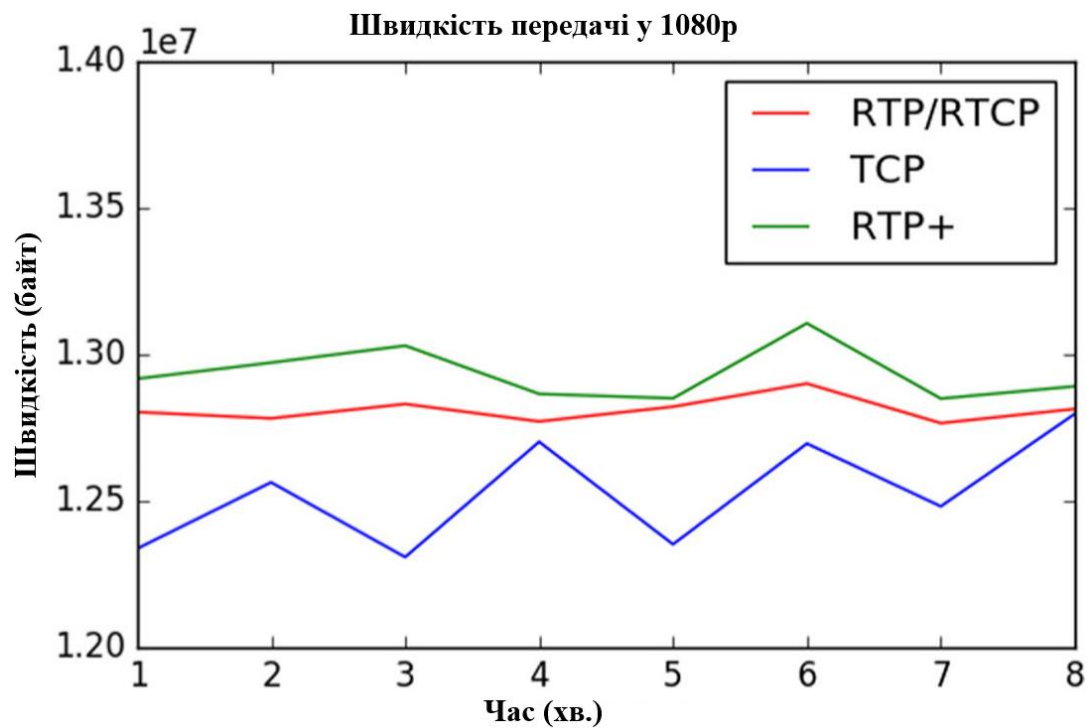
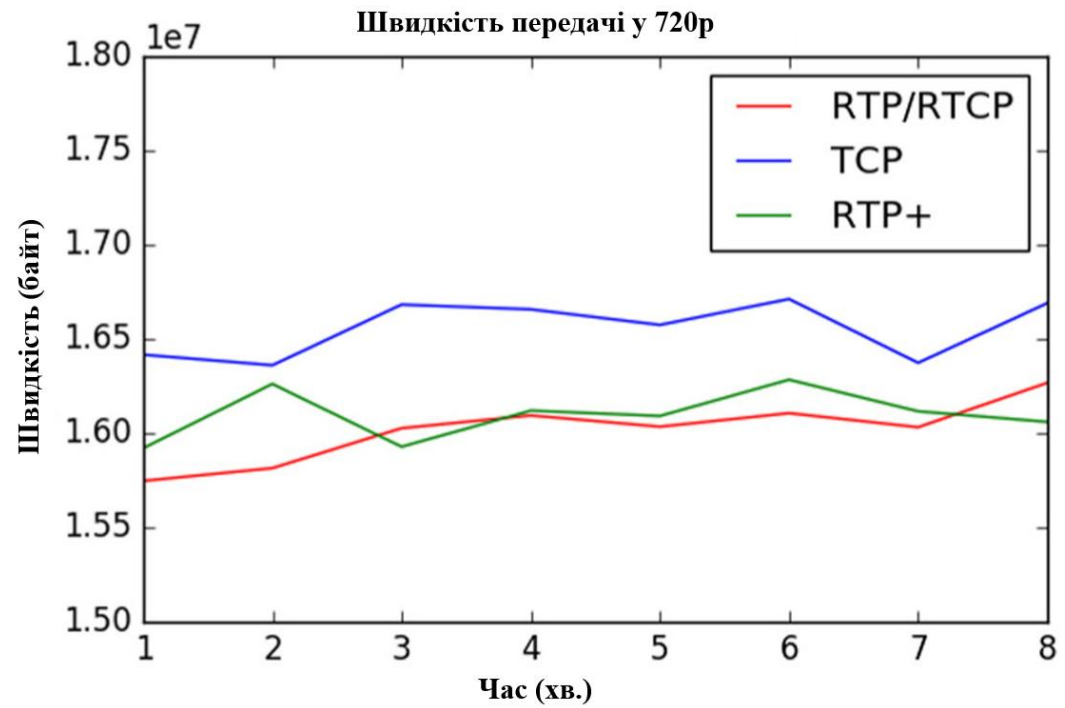


Рисунок 3.7 – Порівняння ефективності передавання за роздільної здатності:
а – 480p, б – 720p, в – 1080p.

Сценарій 2 використовує протокол TCP для передавання, і завдяки механізму TCP швидкість передавання відео повільніша, ніж UDP. Сценарій 1 і сценарій 3 використовують UDP для передавання відео, тому швидкість передачі відео вища. Алгоритм має очевидні переваги перед сценою 2.

Для передавання відео в сценарії 1 і сценарії 3, сценарій 3 повинен повторно передавати ключовий кадр, якщо ключовий кадр втрачено, тому середня швидкість передавання нижче, ніж у сценарії 1. Крім того, як сценарій 1, так і сценарій 3 містять команди управління, з яких в сценарії 1 використано RTCP для надання інформації зворотного зв'язку про передавання даних, а сценарій 3 інформує відправника про повторну передавання втрачених даних, якщо ключовий кадр втрачено. Пакети протоколу RTCP надсилають з перервами, а запит на повторне передавання ключового кадру надсилають тільки у випадку втрати ключового кадру. Отже, в керуючій інформації розмір даних, що передано в сценарії 3, менший, ніж в сценарії 1.

Звичайно, мережеве середовище має великий вплив на порівняння швидкості передавання. У дуже поганому мережевому середовищі, якщо кількість втрат RTP-пакетів є частою, то можливість втрати ключового кадру стане більшою, і кількість повторних передавань збільшиться. Якщо запит на повторне передавання реалізовано за протоколом UDP, запит на повторне передавання може бути втрачений через погану мережу, що призводить до зменшення ключового кадру, який дійсно може бути повторно переданий, тому ефективність цього алгоритму майже аналогічна сцені 1.

3.8 Безпека передавання

В експерименті дослідників [27] вихідні відеоредакти та результат вставки кадрів наведено на рис. 3.8. В даному випадку кадри з номерами а та б є підробленими кадрами, вставленими в кадрове розташування між кадрами 6 та 7. В таблиці 3.1 наведено час розрахунку токена з різними кадрами та роздільною здатністю. Результат полягає в тому, що цей метод, який

дозволяє виявити токен, згенерований приймачем, не відповідає токenu в пакеті. При цьому час обчислення маркера позитивно корелює з кількістю кадрів і розміром роздільної здатності в оригінальному відео, як показано в таблиці 3.1.



Рисун ок3.8 – Вихідний відеоряд і результат вставки кадрів.

Таблиця 3.1

Σ кадрів оригінального відео	Роздільна здатність	Розрахунок часу (с)
152	480p	~0.98
	720p	~1.95
	1080p	~3.14
336	480p	~3.33
	720p	~5.41
	1080p	~7.86

Висновок до розділу

Якість передавання відео в реальному часі часто порушується через нестабільність процесів в довкіллі, а безпека відео в реальному часі може бути втрачена, якщо фальшиве зображення буде долучено у відео під час передавання. Відповідно до інформації про кодування відео та умов безпроводової мережі, на підставі відомого експерименту наведено

докладну інформацію особливостей процесу приймання та відтворення відеопотоку в режимі реального часу та процесу повторного складання отриманого пакету даних на приймальному кінці. Новий алгоритм використовував хеш-таблицю для кешування пакету даних, здійснював ретрансляцію ключового кадру для відсутнього пакету, після чого використовував механізм ковзного вікна для обробки відеосигналу. Відповідно до положення різниці між серійним номером розпакування та серійним номером отриманого пакета у вікні, можна обробити аномалію і виявити вставку при передаванні відео. Перевага цього алгоритму від традиційного методу, який використовував мітку часу та серійний номер для сортування пакета, в тому що він може гарантувати точність та впорядкувати процес сортування відеопакетів та швидко завершити процес послідовного розпакування та відтворення. Також проаналізовано відомий новий метод, заснований на токені, пов'язаний з часом, для забезпечення безпеки передачі відео в реальному часі. В процесі приймання пакетів приймач перевіряє, чи відповідає токен в пакеті власному розрахованому токenu, і може виявити підробку відео при виникненні атаки.

Результати експериментів показують, що відомий новий алгоритм не тільки покращує чіткість відео у випадку відмінного мережевого середовища, але також покращує відтворення відео в поганому мережевому середовищі, такому як мобільне термінальне обладнання та безпроводова мобільна мережа, а й мережеві сигнали відправлення та приймання погані. Швидкість і точність алгоритму мають очевидний ефект. Але, коли пропускна здатність погана, це призведе до збільшення затримки передачі даних. Час передавання кожного відеокадру довший, і коли час передачі перевищує час очікування відтворення відео, це призведе до зупинки кадру на екрані та очікування буфера даних. У таких випадках ретрансляції ключових кадрів в алгоритмі можуть посилити перевантаження мережі, що призведе до збільшення затримки і це треба враховувати.

Таким чином, для забезпечення ефективного функціонування безпроводових систем безпеки в разі застосування такого методу та алгоритму, до особливостей апаратного забезпечення слід долучити вимоги до відеокамер щодо високої роздільної здатності.

4. РОЗРОБКА СТАРТАП-ПРОЄКТУ

4.1 Основна ідея стартап – проєкту.

Головною ідеєю стартап проєкту є реалізація охоронної компанії, що спеціалізується на встановленні охоронних систем безпеки, наглядає за об'єктом через відео моніторинг та втручається при необхідності. В таблиці 4.1 наведено базові ідеї стартапу, напрямки його застосування та вигоду для кінцевого користувача.

Структурно – компанія буде використовувати вже готові рішення на ринку. Винятковою відмінністю від конкурентів буде реалізація алгоритму передачі відеоконтенту по айпі камерам, завдяки якому буде легше та більш наглядно виявити злочинні дії.

Таблиця 4.1

Зміст ідеї	Напрямок застосування	Вигоди для користувача
Розробка бізнес-плану для реалізації охоронного бюро, використання алгоритму передачі відеоконтенту.	Охоронна структура, для користувачів середнього – високого класу, охорона бізнеса.	Зручність у користуванні, професійне встановлення та обслуговування техніки. Додаткові можливості інтеграції охоронних пристроїв, що не входять у пакет комплекту обладнання для охорони.

4.2 Аналіз ринку і конкурентів.

Для подальшого створення стартап-проєкту потрібно проаналізувати ринок України та визначити конкурентів, які можуть негативно вплинути на просування та реалізацію. Також, це допоможе визначитись з цінниками і оптимально розрахувати середню собівартість роботи, найму, оренди та щомісячну квоту обслуговування. Для об'єктивного порівняння обраний один напрям охоронної спеціалізації, а саме – охорона будинків та квартир. Враховуватимуться такі показники для порівняння, як: мінімальна ціна комплекту, вартість встановлення охоронної системи, вартість обслуговування в місяць. Також, потрібно звернути увагу на те, що кожна з представлених фірм, крім ПП «Альянс Безпека» використовують комплекти

безпроводових систем безпеки компанії «AJAX Systems», що і планується в реалізації даного стартап-проєкту. У таблиці 4.2 вказано наглядне порівняння декількох охоронних фірм з їх прайс-листами.

Таблиця 4.2

Назва фірми	Мінімальна ціна комплекту, грн.	Вартість встановлення, грн.	Вартість обслуговування в місяць, грн.
ПП «Ефорт»	8 000	1 500	300
ПП «Комсервіс – Безпека»	7 500	1 000	300
ПП «Охорона і Безпека»	-	-	350
ПП «Альянс Безпека»	3 000	550	150
ПП «Альфа Щит»	6 000	-	200

Згідно з аналізу таблиці 4.2 можна зробити висновок, що деякі компанії роблять націнку на стартові комплекти, беруть гроші за встановлення спеціалістом та мають вартість обслуговування в межах від 150 до 350 гривень. З цього можна зробити висновок, що на старті стартап-проєкту, не беручи націнку за продаж комплектів захисту та з їх безкоштовним встановленням, можна конкурувати на ринку не підвищуючи вартість обслуговування на місяць вище 150 – 200 гривень.



Рисунок 4.1 – SWOT-аналіз стартап-проєкту.

На рис. 4.1 вказано проведений SWOT-аналіз, з якого можна дізнатись про сильні, слабкі сторони стартапу, також можливості його покращення в майбутньому та загрози провалу бізнесу. Такий аналіз може допомогти в розумінні своїх слабкостей та вчасно змінити напрямок розвитку для максимальної вигоди.

Також, аналіз ринку показав, що більшість компаній, які використовують базові безпроводові системи компанії «AJAX Systems» не завжди інтегрують в систему камери відеонагляду, або, роблять це окремо та навіть використовуючи проводові технології, що робить стартап більш унікальним на фоні конкурентів.

З мінусів, звичайно, неможливість на базовому етапі користуватись наймом оперативної служби для невідкладного виїзду на місце злочину, що є у більшості конкурентів. Також, спектр послуг, який обмежується тільки спостереженням та вчасною подачею інформації в спеціальні органи безпеки держави, відповідно, лише охороною об'єктів під наглядом, тривожними кнопками, та різними датчиками.

4.3 Визначення цільової аудиторії.

Для визначення цільової аудиторії слід проаналізувати декілька факторів. Найважливіший з них – потреба в охороні об'єктів. Якщо враховувати охорону будівель, жилих домів та квартир, то цільовою аудиторією вважається люди середньо-високого капіталу, так як в них є певні збереження та цінні речі, які можуть бути ціллю для нападу грабіжників та зловмисників. Щодо приватних підприємців – кожен може бути клієнтом даного стартап проекту, так як кожен бізнес потребує нагляду і охорони.

Також фактором, що може вплинути на потенційного клієнта є саме можливість встановлення безпроводових систем безпеки. Такими переважно є молоді чоловіки та жінки 30 років якщо аналізувати в середніх вікових межах.

Отже, цільова аудиторія даного стартап-проекту – чоловіки та жінки з середнім віком – 30 років, середньо – високого капіталу з потребою в охороні нерухомості.

4.4 Опис мінімально життєздатного продукту.

Мінімально життєздатний продукт являтиме собою офіс, бажано в центрі району або мікрорайону. Основними поставками для даного бізнесу на основі стартап-проекту будуть вироби компанії «AJAX Systems», в повному обсязі продукції, закупка необхідних датчиків та хабів відбуватиметься на замовлення. Також, як рішення для встановлення безпроводових камер відеонагляду використовуватиметься продукція компанії «Hikvision», так як вони підходять для під'єднання до безпроводових систем запропонованих Аякс системс.

Компанія надаватиме послуги закупівлі продукції, її встановлення у приміщення, налаштування компонентів та їх обслуговування. Також, забезпечить зв'язок з державними органами для оперативного виїзду на місце вторгнення або при стихійних втручаннях.

Особливість такої компанії в тому, що при мінімальних вкладеннях користувача буде забезпечена максимально можлива система захисту з моніторингом, чого має вистачити насамперед тим, хто не готовий платити великі гроші за оперативну групу, але хоче мати моніторинг місцевості та страхування від проблем вторгнень.

Для роботи компанії достатньо мати одну людину, яка може непогано справлятися, особливо на початку, коли клієнтура буде маленькою. Робітнику буде надано машину для невідкладних виїздів при виходу з ладу техніки, надання сервісного обслуговування на дому та, насамперед, встановлення системи.

В таблиці 4.3 проаналізовано за скільки часу можна окупити даний стартап-проект.

Таблиця 4.3

Витрати на місяць за перший рік												
Офіс	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.
Зарплатня працівнику	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.
Обслуговування транспорту	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.
Комунальні платежі	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.
Отримані кошти з клієнтів	4 000 грн.	6 000 грн.	8 000 грн.	10 000 грн.	12 000 грн.	14 000 грн.	16 000 грн.	18 000 грн.	20 000 грн.	22 000 грн.	24 000 грн.	26 000 грн.
Всього, грн.	-17 340	-28 680	-42 020	-55 360	-68 700	-82 040	-95 380	-108 720	-122 060	-121 400	-118 740	-114 080
Витрати на місяць за другий рік												
Офіс	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.
Зарплатня працівнику	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.
Обслуговування транспорту	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.
Комунальні платежі	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.
Отримані кошти з клієнтів	28 000 грн.	30 000 грн.	32 000 грн.	34 000 грн.	36 000 грн.	38 000 грн.	40 000 грн.	42 000 грн.	44 000 грн.	46 000 грн.	48 000 грн.	50 000 грн.
Всього, грн.	-110 753	-107 093	-103 433	-99 773	-96 113	-92 453	-88 793	-85 133	-81 473	-77 813	-74 153	-70 493
Витрати на місяць за третій рік												
Офіс	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.
Зарплатня працівнику	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.
Обслуговування транспорту	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.
Комунальні платежі	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.
Отримані кошти з клієнтів	52 000 грн.	54 000 грн.	56 000 грн.	58 000 грн.	60 000 грн.	62 000 грн.	64 000 грн.	66 000 грн.	68 000 грн.	70 000 грн.	72 000 грн.	74 000 грн.
Всього, грн.	-66 833	-63 173	-59 513	-55 853	-52 193	-48 533	-44 873	-41 213	-37 553	-33 893	-30 233	-26 573
Витрати на місяць за четвертий рік												
Офіс	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.	8 704 грн.
Зарплатня працівнику	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.	6 700 грн.
Обслуговування транспорту	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.	5 000 грн.
Комунальні платежі	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.	936 грн.
Отримані кошти з клієнтів	76 000 грн.	78 000 грн.	80 000 грн.	82 000 грн.	84 000 грн.	86 000 грн.	88 000 грн.	90 000 грн.	92 000 грн.	94 000 грн.	96 000 грн.	98 000 грн.
Всього, грн.	-22 913	-19 253	-15 593	-11 933	-8 273	-4 613	-953	2 707	6 367	10 027	13 687	17 346

Як можна побачити, даний стартап при стабільних зовнішніх умовах може окупитись за три роки і вісім місяців, що є дуже непоганим результатом в умовах нашої держави.

Висновки до розділу

В даному розділі було проаналізовано можливість створення стартап-проєкту, в основі якого лежить ідея формування охоронного бюро низького бюджету. Під час аналізу досліджено сильні та слабкі сторони проєкту, конкуренція та конкурентоспроможність, проаналізовано ринок, визначено уявне розташування офісу, напрямки роботи, кількість персоналу, необхідні плани для успішного старту та роботи бізнесу в майбутньому.

При аналізі ринку з'ясовано, що конкуренти беруть націнки і встановлюють високий поріг цін так як мають широкий вплив на території міста, використовують фізичні способи охорони. Такі компанії в основному існують на ринку України і з ними можна конкурувати з рахунок дешевизни обслуговування на місяць та розуміння того, що не кожному потрібний такий рівень захисту нерухомості.

Також проаналізовано окупність даного стартап-проєкту, зсилаючись на теоретичні можливі способи витрат та щомісячного стабільного приросту

клієнтури. Таким чином, згідно статистики, окупитись стартап може за три роки та вісім місяців, що є досить хорошим результатом.

Отже, такого роду стартап-проекти мають право на існування в сучасному світі, але треба враховувати певні серйозні недоліки. По перше – малий бізнес в Україні дуже важко реалізувати, із за високих податків та впливу конкурентів. По друге – монополізація. На жаль, навіть створені бюро та сегменти влади по боротьбі з монополізацією не завжди дають гарантію на безпеку малим та середнім бізнесам. По третє – потрібно завжди слідкувати за трендами ринку та за тим як він працює, так як ситуація може змінитись кожен день.

ВИСНОВКИ

У даній роботі досліджено особливості сучасного апаратного забезпечення безпроводових систем безпеки. В ході дослідження проаналізовано сучасний ринок систем безпеки, різницю між проводовими та безпроводовими рішеннями, виявлено конкретні переваги і недоліки.

1.Безпроводові рішення підходять там, де необхідно використовувати систему безпеки у вже сформованій сфері та є можливість розширення щодо кількості датчиків і системи в цілому, для споживачів, які не планують полишати територію що охороняється на дуже великі проміжки часу, так як всі БСБ працюють на батарейках.

2. Для коректної роботи безпроводові системи безпеки використовують різноманітні протоколи передавання інформації. Всі вони мають певні стандарти та зроблені так, щоб не перебивати сигнал і не створювати шум для інших елементів системи або навколишнього середовища. Найкращою компанією на ринку України з виготовлення безпроводових систем безпеки і однозначним лідером є компанія Ajax systems. Також, системи безпеки компанії є лідерами у різноманітності датчиків для системи безпеки та мають унікальний протокол передачі інформації, що погіршує шанс доповнити систему іншими пристроями сторонніх виробників але водночас робить її унікальною. Ціна на системи є нормальною, зважаючи на набори датчиків.

3. При використанні безпроводових технологій, таких як системи безпеки, також існують проблеми зі збуреннями, як штучними так і природніми. Щоб захистити систему від штучних збурень створено багатоканальні системи, що мінімізує ризик виводу з ладу системи. Від природніх же – спеціалізована техніка яка може витримати різноманітні тяжкі погодні умови, такі як спека або холод.

4. Для аналізу пристроїв та симуляцій збурень та роботи існує безліч програмного забезпечення. Кожне ПЗ є унікальним та підходить в окремих

задачах. Найбільш функціональна з них – програма від компанії MATLAB, так як має широкий спектр для використання, має синергію з програмним забезпеченням SimuLink, що дозволяє не змінювати декілька варіантів середовищ і з'єднувати програмування з симуляцією в реальних умовах.

4. На підставі аналізу протоколів передавання інформації використовуючи айпі-камери та методів покращення технологію передавання пакетів, для забезпечення ефективного функціонування безпроводових систем безпеки в разі застосування методу та алгоритму за публікацією [27], до особливостей апаратного забезпечення слід долучити вимоги до відеокамер щодо високої роздільної здатності, це зменшить витрати та дозволить стабілізувати відеоряд між відправником та отримувачем. Результати відомих експериментів показали, що є алгоритм, який не тільки покращує чіткість відео у випадку відмінного мережевого середовища, але також покращує відтворення відео в поганому мережевому середовищі, такому як мобільне термінальне обладнання та безпроводова мобільна мережа, а й мережеві сигнали відправки та приймання погані. Швидкість і точність алгоритму мають очевидний ефект. Але, коли пропускна здатність погана, це призведе до збільшення затримки передачі даних. Однак час передачі кожного відеокадру довший, і коли час передавання перевищує час очікування відтворення відео, це призведе до зупинки екрану та очікування буфера даних. Це перевантажить мережу, що призведе до збільшення затримки і на це також треба зважати.

В останньому розділі було проаналізовано можливість створення стартап-проєкту, в основі якого лежить ідея формування охоронного бюро низького бюджету. Під час аналізу досліджено сильні та слабкі сторони проєкту, конкуренція та конкурентоспроможність, проаналізовано ринок, визначено уявне розташування офісу, напрямки роботи, кількість персоналу, необхідні плани для успішного старту та роботи бізнесу в майбутньому.

СПИСОК ЛІТЕРАТУРИ

1. De Koning Gans Gerhard, Hoepman J.-H., Garcia F.D. A practical attack on the MIFRARE Classic // 8th Smart Card Research and Advanced application Workshop (CARDIS 2008), LNCS, Springer.
2. Courtois Nicolas T., Karsten Nohl, Sean O'Neil. Algebraic attack on the Crypto 1 Stream cipher in MIFRARE classic and Oyster cards. Cryptology ePrint Archive.
3. Garcia Flavio D., de Koning Gans Gerhard, Muijrs Ruben, van Rossum Peter, Verdult Roel, Schreur Ronny Wichers, Jacobs Bart. Dismantling MIFRARE Classic // 13th European symposium on research in computer security (ESORISC 2008), LNCS, Springer.
4. Garcia Flavio D., van Rossum Peter, Verdult Roel, Schreur Ronny Wichers. Wirelessly pickpocketing a mifrare classic card // 30th IEEE Symposium on security an privacy (S&P 2009), IEEE.
5. Eisenbarth Thomas, Kasper Timo, Moradi Amir, Paar Christof, Salmasizadeh Mahammad, Shalmani Mohammad T. Manzuri. Physical cryptanalysis of KeeLogCode Hopping applications. Ruhr university of Bochum, Germany/ Retired 2009-03-22.
6. Novotny Martin, Kasper Timo. Cryptanalysis of keeLoq with COPOCOBANA, SHARCS 2009 Conferece.
7. Scarfone Karen, Padgett John. Guide to Bluetooth security // NIST special publication sep. 2008.
8. ISO/IEC 26907 Information technology — Telecommunications and information exchange between systems — High-rate ultra-wideband PHY and MAC standard.
9. IEEE 802.15.4 IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks — Specific requirements.

10. Buttyran L., Czap L., Vajda I. Securing coding based distributed storage in wireless sensor networks // Proceedings of the IEEE Workshop on Wireless and Sensor Network Security (WSNS), Atlanta, USA, 2008.
11. Lima L., Vilela J., Oliveira P., Barros J., Filiz I., Guo X., Morton J., Sturmfels B., Mungan M., Ramasco J. [et al.] Network Coding Security Attacks and Countermeasures. 2008.
12. Jaggi S., Langberg M., Katti S., Ho T., Katabi D., Mredard M. Resilient network coding in the presence of byzantine adversaries // Proceedings of the Conference of the IEEE Computer and Communications Societies (INFOCOM), Anchorage, Alaska, USA, 2007. P. 616–624.
13. Buttyran Levente, ro Czap Lraszl, Vajda Istvan. Pollution Attack Defense for Coding Based Sensor Storage Proceedings of the Conference of the IEEE Computer and Communications Societies (INFOCOM), Anchorage, Alaska, USA, 2010.
14. Dong J., Curtmola R., Nita-Rotaru C. Practical defenses against pollution attacks in intraflow network coding for wireless mesh networks, in WiSec '09 // Proceedings of the second ACM conference on Wireless network security. New York, NY, USA: ACM, 2009. – P. 111– 122.
15. Courtois N. Efficient zero-knowledge authentication based on a linear algebra problem minrank // Proceedings of ASIACRYPT, 2001. – P. 402–421.
16. Cai N., Yeung R. Secure network coding // Proceedings of the IEEE International Symposium on Information Theory. Lausanne, Switzerland. 2002.
17. Cai N., Yeung R. Network error correction // Proceedings of the IEEE International Symposium on Information Theory, Yokohama, Japan, July. 2003.
18. Cai N., Yeung R. W. A Security Condition for Multi-Source Linear Network Coding // IEEE International Symposium on Information Theory (ISIT). Nice, France. 2007.

19. Lima L., Vilela J. P., Barros J., Medard M. 2008. An Information-Theoretic Cryptanalysis of Network Coding — is protecting the code enough? // International Symposium on Information Theory and its Applications, ISITA2008. Auckland, New Zealand.
20. What Are The Different Types of Security Systems? [Електронний ресурс] // Safeguard Security Systems Ltd, 2022. URL: <https://safeguardsystems.co.uk/security-systems-news/different-types-security-systems/> (дата звернення: 27.10.2022)
21. Провідні бренди ринку систем безпеки [Електронний ресурс] // BEZPEKA.CLUB Ltd, 2022. URL: <https://bezpeka.club/ua/brands/>
22. Бездротові охоронні пристрої системи безпеки Ajax [Електронний ресурс] // AJAX SYSTEMS CH Ltd, 2022. URL: <https://ajax.systems/ua/products/jeweller/>
23. Що таке глушіння бездротової системи безпеки та як йому протистояти [Електронний ресурс] // AJAX SYSTEMS CH Ltd, 2022. URL: <https://ajax.systems/ua/blog/what-is-jamming/>
24. Чим відрізняється професійна система безпеки від дешевої сигналізації [Електронний ресурс] // AJAX SYSTEMS CH Ltd, 2022. URL: https://ajax.systems/ua/blog/differences_of_professional_systems/
25. MATLAB – офіційна сторінка [Електронний ресурс] // 2022 The MathWorks, Inc. URL: <https://www.mathworks.com/products/matlab.html>
26. LabView – офіційна сторінка [Електронний ресурс] // 2022 NATIONAL INSTRUMENTS CORP. URL: <https://www.ni.com/en-us/support/downloads/software-products/download.labview.html#460283>
27. Improving the security and quality of real-time multimedia transmission in cyber-physical-social systems//Qindong Sun, Han Cao, Wenjing Qi and Jingpeng

Zhang// International Journal of Distributed Sensor Networks, 2018, vol. 14, issue 11, DOI: 10.1177/1550147718810694

ДОДАТОК А
SUMMARY

Today there are many security systems for different needs of mankind. It can be anything from video cameras in shopping centers and parking lots to high-tech military structures where critical information, weapons and explosives are stored. That is, these systems vary depending on the degree of importance and possible risks. Sometimes a few motion detectors and an ordinary alarm system may be enough, and sometimes an armored area with metal wire around the perimeter, warning signs, searchlights, security turrets, etc. is required. In both the first and second examples, these can be classified as security systems.

People have long dreamed of wireless technology, as most often, wires create a lot of fuss. They are bulky, tangled with each other, they have a length that is often not enough, and there is not much aesthetics in wired connections. That is why the study of information transmission between devices through the "air" was a very urgent problem. In the modern world, science has already found a way out and you can buy a smartphone, laptop, and many other wireless technologies in the open market. The same is the technology that is the main one for discussion in this paper.

Wireless security systems are the youngest technologies that are offered to the user. They have their pros and cons, some of them obvious and some not as predictable as it seems at first glance. In this paper we consider modern technologies of wireless security systems and how they work, market analysis and possible solutions, both in Ukraine and in the world, topology of information transmission, method of transmission and general operation of security systems.

This paper investigates the features of modern hardware of wireless security systems. In the course of the study, the modern market of security systems, the difference between wired and wireless solutions were mastered, specific pros and cons were identified. Namely, wireless solutions are suitable for those who want to use the security system in the already established real estate and intend to expand the sensors and the system as a whole, who do not plan to leave the protected area for very long periods of time, since all the BSBs work on batteries, those who like

modern solutions and the elegance of wireless devices. For correct operation, wireless security systems use a variety of information transfer protocols. All of them have certain standards and are made so as not to interrupt the signal and not to create noise for other elements of the system or the environment. The best company in the Ukrainian market for the production of wireless security systems and the undisputed leader is Ajax systems. Also, the company's security systems are leaders in the variety of sensors for the security system and have a unique protocol for transmitting information, which reduces the chance to supplement the system with other third-party devices but at the same time makes it unique. The price of the systems is normal, given the sets of sensors.

When using wireless technologies, such as security systems, there are also problems with disturbances, both artificial and natural. To protect the system from artificial disturbances, multi-channel systems have been created to minimize the risk of system failure. From natural ones - specialized equipment that can withstand a variety of severe weather conditions, such as heat or cold.

There is a variety of software available to analyze devices and simulate disturbances and operation. Each software is unique and suitable for specific tasks. The most functional of them is the program from MATLAB company, as it has a wide range for use, has synergy with SimuLink software, which allows not to change several variants of environments and to connect programming with simulation in real conditions.

The third section investigates the protocols of information transmission using IP cameras and improve the technology of packet transmission, reduce losses and stabilize the video sequence between sender and receiver. Experimental results show that the proposed algorithm not only improves the video clarity in the case of excellent network environment, but also improves the video display in poor network environment such as mobile terminal equipment and wireless mobile network, and the network signals of sending and receiving are poor. The speed and accuracy of the algorithm have an obvious effect. But, when the bandwidth is poor,

it will cause the data transmission delay to increase. The transmission time of each video frame is longer, and when the transmission time exceeds the video display waiting time, it will cause the screen to stop and wait for the data buffer. In such cases, retransmissions of key frames in the algorithm can increase the network congestion, which will lead to an increase in latency and this should be taken into account.

In the last section, the possibility of creating a startup project based on the idea of forming a low-budget security bureau was analyzed. During the analysis, the strengths and weaknesses of the project, competition and competitiveness were investigated, the market was analyzed, the imaginary location of the office, the direction of work, the number of staff, the necessary plans for a successful start and operation of the business in the future were determined.