ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОМПОНЕНТІВ IoT СИСТЕМИ ОХОРОНИ ПЕРИМЕТРУ РЕЖИМНОГО ОБ'ЄКТУ»

Виконала студентка 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Лобанчикова Н.М.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"01" жовтня 2020 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Лобанчиковій Надії Миколаївні
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія забезпечення кібербезпеки компонентів IoT системи охорони периметру режимного об'єкту»

керівник магістерської роботи Гайдур Галина Іванівна, д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «13» жовтня 2020 року № 230.

2. Строк подання студентом магістерської роботи 15.12.2020 р.

3. Вихідні дані до магістерської роботи
опис типових систем охорони периметру; типовий склад IoT систем; змінна територія об'єкту; відсутність електроенергії; апаратне та програмне забезпечення; енергонезалежність протягом 24 годин; наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження компонентів систем охорони периметру
2. Моделювання IoT системи охорони периметру
3. Дослідження технологій кіберзахисту компонентів IoT системи
Висновки з проведеного дослідження

5. Перелік графічного матеріалу
Комп'ютерна презентація за результатами дослідження

6. Дата видачі завдання 01.10.2020 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності технологій забезпечення кібербезпеки компонентів IoT систем охорони периметру	09.10.2020 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	30.10.2020 р.	
3.	Моделювання IoT системи охорони периметру	16.11.2020 р.	
4.	Реалізація IoT системи охорони периметру засобами комп'ютерного моделювання	23.11.2020 р.	
5.	Аналіз кіберзагроз на компоненти IoT-системи та розробка рекомендацій.	02.12.2020 р.	
6.	Оформлення результатів дослідження.	09.12.2020 р.	
7.	Підготовка доповіді до захисту.	15.12.2020 р.	

Студент Лобанчикова Н.М.
(підпис) прізвище та ініціали

Керівник магістерської роботи Гайдур Г.І.
(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 81 сторінці, 41 рисунок, 31 джерело.

Об'єкт дослідження: процес забезпечення кібербезпеки компонентів IoT системи охорони периметру.

Предмет дослідження: моделі, методи, засоби та технології забезпечення кібербезпеки компонентів IoT систем охорони периметру

Метою дослідження є вирішення важливої науково-технічної задачі підвищення рівня кібербезпеки систем охорони периметру режимних об'єктів суттю якої є розробка технології забезпечення кібербезпеки компонентів IoT системи охорони периметру.

Методи дослідження – в роботі було використано методи теорії систем та системного аналізу, методи комп'ютерного проектування та моделювання. Інформаційну базу дослідження складають: інформаційно-аналітичні матеріали, статистичні дані використання розумних датчиків підприємствами опубліковані у періодичних та спеціалізованих виданнях, підходів до реалізацій поставленої задачі, а також матеріали розміщенні у мережі Інтернет.

Аналіз криміногенної ситуації свідчить про зростання кількості крадіжок, вандалізму, спроб несанкціонованого доступу до території об'єктів охорони. Особливо актуально питання ставить при охороні режимних об'єктів, що є потенційно цікавими для терористів та певних кримінальних угрупувань. Широке впровадження та розвиток IoT систем призвели до виникнення нових типів кіберзагроз. Тому дослідження технологій захисту і забезпечення кібербезпеки компонентів IoT систем є актуальною задачею сьогодення.

В першому розділі проведено аналіз засобів виявлення в системах охорони периметру, аналіз мобільних засобів охорони та особливості їх застосування, аналіз методів ідентифікації особи, аналіз проблеми забезпечення кібербезпеки компонентів IoT систем.

В другому розділі запропоновано структурну модель IoT системи охорони периметру засобами комп'ютерного моделювання, модель прояву порушників на території об'єкту охорони, метод побудови блоку прийняття рішень із виявлення несанкціонованого доступу. Проведено реалізацію IoT системи охорони периметру засобами комп'ютерного моделювання.

В третьому розділі проведено аналіз кіберзагроз на компоненти IoT системи, розроблені рекомендації з протидії атакам на компоненти IoT системи, запропоновано модель підсистеми моніторингу інцидентів кібербезпеки в IoT системах.

Галузь використання – кібербезпека корпоративних інформаційних систем.

АТАКА, БЕЗПЕКА, IoT СИСТЕМА, ІНТЕРНЕТ РЕЧЕЙ, КІБЕРБЕЗПЕКА, ОХОРОНА ПЕРИМЕТРУ, СЕНСОРНІ МЕРЕЖІ, ТЕХНОЛОГІЯ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

МО – Міністерство оборони

НСД – несанкціонований доступ

ПЗВ – периметрові засоби виявлення

ПЗ – програмне забезпечення

ПКІ – переносний пульт керування й індикації

РЛС – радіолокаційна станція

РЛСП – радіолокаційна система пошуку

РЛСР – радіолокаційна система розвідки

СМЗ – система мобільного захисту

СППР – система підтримки прийняття рішень

ТЗО – технічні засоби охорони

ТРВО – тимчасово розташовані військові об’єкти

ШвР – швидкого розгортання

AES – Advanced Encryption Standard – симетричний алгоритм блочного шифрування

CTS – Clear to Send

DoS – Denial-of-Service – відмова в обслуговуванні

IoT – Internet of Things – інтернет речей

RFID – Radio Frequency IDentification – радіочастотна ідентифікація

RTS – Ready to Send

TCP – Transmission Control Protocol – протокол керування передачею

UDP – User Datagram Protocol – Протокол датаграм користувача

ВСТУП

Актуальність дослідження. Аналіз криміногенної ситуації свідчить про зростання кількості крадіжок, вандалізму, спроб несанкціонованого доступу до території об'єктів охорони. Особливо актуально питання ставить при охороні режимних об'єктів, що є потенційно цікавими для терористів та певних кримінальних угрупувань. Все частіше постає питання про тимчасовий захист об'єктів при перевезенні озброєння, техніки, радіоактивних відходів та матеріалів, проведенні розвідувальних операцій в зоні проведення антитерористичної операції. Особливість задачі обумовлена «польовими» умовами функціонування системи, що вимагає ретельного підбору складових системи, підвищення вимог до їх працездатності та точності. Слід зауважити і на тому, що система повинна працювати з урахуванням рельєфу місцевості розгортання, бути непомітною для зловмисників, зручною у використанні, стійкою до параметрів навколишнього середовища та кібератак.

Останні декілька років широко розвитку та впровадження набули IoT системи. Нові технології та нові засоби породжують і нові типи кіберзагроз. Впровадження у повсякденне життя IoT систем та засобів отримало виклик від нових загроз та повинне протистояти все новим і новим викликам. Тому дослідження технологій захисту і забезпечення кібербезпеки компонентів IoT систем є актуальною задачею сьогодення.

Об'єкт дослідження: процес забезпечення кібербезпеки компонентів IoT системи охорони периметру.

Предмет дослідження: моделі, методи, засоби та технології забезпечення кібербезпеки компонентів IoT систем охорони периметру

Метою дослідження є вирішення важливої науково-технічної задачі підвищення рівня кібербезпеки систем охорони периметру режимних об'єктів

суттю якої є розробка технології забезпечення кібербезпеки компонентів IoT системи охорони периметру.

Наукові завдання:

дослідити сутність проблеми забезпечення кібербезпеки компонентів IoT систем;

дослідити технології побудови систем охорони периметру;

проаналізувати існуючі технології забезпечення кібербезпеки компонентів IoT систем охорони периметру;

провести моделювання роботи системи засобами комп'ютерного моделювання у середовищі Cisco Packet Tracer;

розробити технологію забезпечення кібербезпеки компонентів IoT системи охорони периметру

Методи дослідження – в роботі було використано методи теорії систем та системного аналізу, методи комп'ютерного проектування та моделювання. Інформаційну базу дослідження складають: інформаційно-аналітичні матеріали, статистичні дані використання розумних датчиків підприємствами опубліковані у періодичних та спеціалізованих виданнях, підходів до реалізацій поставленої задачі, а також матеріали розміщенні у мережі Інтернет.

Наукова новизна дослідження. До найбільш вагомих наукових результатів слід віднести:

− проведений аналіз технологій забезпечення кібербезпеки компонентів IoT систем охорони периметру;

− запропоновану структурну модель IoT системи охорони периметру, яка являє собою інтеграцію модулів: підсистему безконтактної радіочастотної ідентифікації (RFID), підсистему інтелектуального відеоспостереження, СППР із виявлення несанкціонованого доступу на територію об'єкту охорони, підсистему виявлення руху по контуру периметру захисту;

– рекомендації щодо забезпечення кібербезпеки компонентів IoT систем охорони периметру.

Практичне значення одержаних результатів полягає в розробці IoT системи охорони периметру та розробці прототипу IoT системи засобами комп'ютерного моделювання у середовищі Cisco Packet Tracer.

Особистий внесок здобувача. Усі результати роботи отримані автором самостійно.

Апробація результатів: Основні результати кваліфікаційної роботи доповідалися та обговорювались на таких конференціях: X Міжнародній науково-технічній конференції «Інформаційно-комп'ютерні технології – 2019», XI Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2020 (ІКТ-2020)», at the International Conference on History, Theory and Methodology of Learning (ICHTML ^{2020}).

Публікації. Основні результати магістерської роботи були опубліковані у вигляді 1 статті та 2 тез конференції [1-3]:

1. Лобанчикова Н.М. Модель побудови мобільної систем охорони периметру території / Н. М. Лобанчикова // Сучасний захист інформації: Наук.-техн. журнал.– Київ: ДУТ, 2020. – №1(41). – С.42 – 48.

2. Лобанчикова Н.М., Серденюк Б.О. Дослідження процесів захисту інформації в IoT. Тези доповідей X Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2019», 18-20 квітня 2019 року. Житомир: ЖДТУ, 2019. С. 80-83.

3. Lobanchykova N., Kredentsar S. Methodology for Perimeter Security Systems Creation. Тези доповідей XI Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2020 (ІКТ-2020)», 09 - 11 квітня 2020 року. Житомир: Житомирська політехніка, 2020. С.101-102.

1. ДОСЛІДЖЕННЯ КОМПОНЕНТІВ СИСТЕМ ОХОРОНИ ПЕРИМЕТРУ

1.1. Аналіз засобів виявлення в системах охорони периметру

Режимна територія – земельна ділянка, що охороняється в межах встановлених кордонів, яка обгороджена по периметру парканом або колючим дротом, іноді цегляною або бетонною стіною, обладнана інженерно-технічними засобами охорони, на якій ведуться секретні роботи чи розміщені будівлі (споруди) закладів, що виготовляють зразки озброєння і військової техніки.

Для розробки технології забезпечення кібербезпеки компонентів IoT системи проведемо дослідження засобів виявлення, що використовуються в системах охорони периметру. На теперішній час як вітчизняні, так і закордонні виробники використовують широкий спектр фізичних принципів побудови електронних систем охорони. Найбільш розповсюджені радіохвильові, радіопроменеві, оптичні, ємнісні, вібраційно-чутливі, контактні, сейсмічні, волоконно-оптичні системи та ін., рисунок 1.1. Слід зазначити, що одним з ефективних заходів по забезпеченню безпеки об’єктів є створення автоматизованої системи охорони від несанкціонованого проникнення фізичних осіб [1, 4-10].

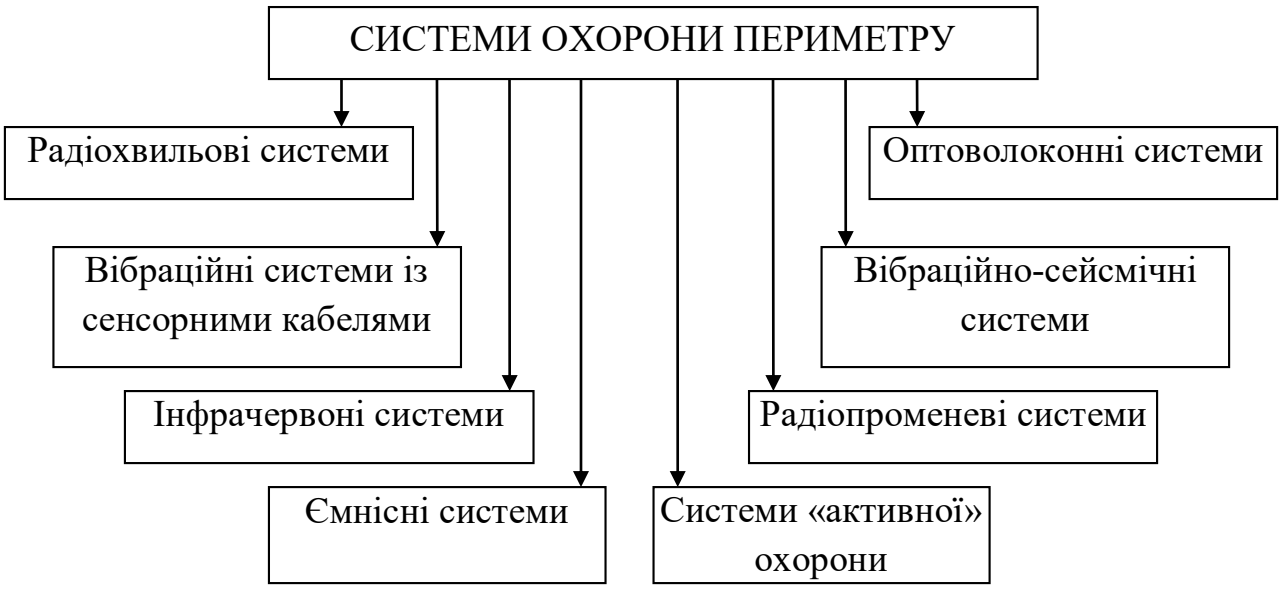


Рис. 1.1. Класифікація систем охорони периметру

Периметрові інженерні загородження служать для огородження територій

військових, промислових, цивільних і спеціальних об'єктів з метою виключення проникнення на них сторонніх осіб і транспортних засобів. Основою периметрового комплексу інженерних споруджень є сітчасте загородження, виконане зі зварної оцинкованої полотнини СЗОП 250/50 з діаметром дроту 3 мм. У периметровий комплекс інженерних споруджень крім сітчастого загородження входять ворота «розпашні» металеві для проїзду транспорту і хвіртка для проходу людей. Конструкція сітчастого загородження передбачає лази для дрібних тварин. Висока стійкість сітчастої оцинкованої полотнини до кліматичних впливів і її висока міцність дозволяють створити довгострокові фізичні перешкоди сучасного типу у всіх кліматичних зонах України. Основним загороджувальним елементом зовнішнього огородження є його полотнина**.** В даний час для зовнішнього огородження використовуються:

1. Глуха полотнина (матеріал: бетонні плити, цегляна кладка, металопрофільні конструкції, металеві зварні чи дерев'яні щити) (див. рис.1.2).

Рис.1.2. Варіант виконання «глухої» полотнини

Це суцільне, монолітне огородження. Воно, як правило, використовується в разі потреби забезпечити високу скритність специфіки діяльності на території об’єкту охорони, режиму його функціонування, виробленої продукції і т.п.

2. Транспортна полотнина (матеріал: дріт, сітка, ґратчасті конструкції з: металу, бетону, цегли, дерева, або сітчасті секції) (див. рис.1.3).

Рис.1.3. Варіант виконання ґратчастої конструкції

Це огородження, як правило, призначається для контурного вигороджування кордонів периметра об’єкта охорони. Розрізняють тверду і гнучку конструкції полотнини [4-10].

З До комбінованих огороджень відносять огородження, у яких при будівництві використовується об’єднання різних типів конструкцій і матеріалу полотнини. Комбінація матеріалу при виготовленні зовнішнього огородження дає можливість підвищити його захисні властивості і знизити при цьому витрати на будівництво й обслуговування.

Засоби сигналізації призначені для раннього виявлення різноманітних несанкціонованих порушень. Для виявлення факту вторгнення порушника в зону охорони можуть бути використані різні фізичні принципи, що дозволяють з тим або іншим ступенем імовірності розрізнити сигнал спричинений діями порушника, на фоні перешкод різного походження. Класифікація периметрових засобів виявлення (ПЗВ) за їхніми фізичними принципами наведена в структурній схемі (див. рис. 1.4).

Слід зазначити, що широке використання технічних засобів охорони (ТЗО) дозволяє виключити або звести до мінімуму негативний вплив самої ненадійної ланки в системі охорони – людини. Людині в процесі тривалого чергування властиві стомлюваність, неуважність, навіть недбалість. При цьому, організація охорони за допомогою ТЗО обходиться значно дешевше, а надійність при цьому

підвищується. Тому як вітчизняні, так і закордонні виробники, приділяють велику увагу створенню ТЗО на основі останніх наукових досягнень інформаційних і комунікаційних технологій.

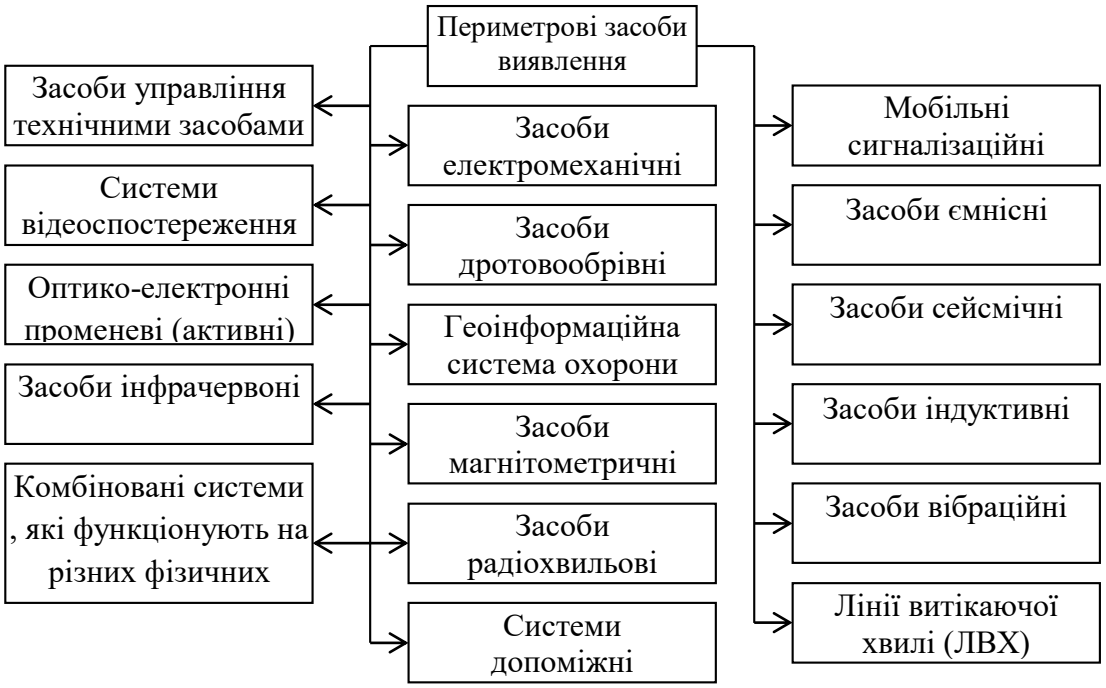


Рис.1.4. Класифікація периметрових засобів виявлення за їх фізичними принципами дії

Тенденції розвитку сучасних периметрових засобів виявлення спрямовані на: зниження собівартості датчиків і чутливих елементів; підвищення тактико-технічних характеристик; підвищення надійності; підвищення довговічності; зниження частоти помилкових спрацювань; підвищення завадостійкості та ін.

В теперішний час здійснюється перехід на цифрову обробку сигналів на основі мікропроцесорної техніки, що забезпечує компенсацію впливу зовнішніх факторів, розпізнавання типових сигналів, автоматичну діагностику і настроювання датчиків під конкретні умови експлуатації. Упровадження цифрових методів обробки дозволяє одержати принципово нові якісні характеристики системи охорони в цілому, забезпечити велику імовірність виявлення на фоні численних зовнішніх і дестабілізуючих факторів, створити клас інтелектуальних датчиків, які

самонавчаються, що адаптуються до конкретних умов експлуатації при збереженні високих сигналізаційних характеристик.

В даний час у деяких країнах проводяться розробки мобільних сигналізаційних комплексів. Системи такого типу мають малі габарити, вагу й енергоспоживання, що дозволяє забезпечити приховану і швидку установку на рубежі, що охороняється, навіть на непідготовлених в інженерному відношенні ділянках пересічної і лісистої місцевості. Вони можуть застосовуватися на окремих ділянках периметрів об'єктів, обладнаних стаціонарними системами, у період їхнього ремонту або надзвичайних ситуацій. Тактико-економічні характеристики мобільних комплексів, можливість створення на їхній основі систем мобільного захисту (СМЗ) без виконання трудомістких проектних і будівельно-монтажних робіт, а також можливість оперативної зміни, у разі потреби, конфігурації контрольованого рубежу, робить їх привабливими для використання при рішенні задач у системах охорони стаціонарних об'єктів. Це стає можливим при невеликих змінах конструкції їхніх монтажних частин.

Найбільш відомі системи охорони периметру:

- «РАДІЙ-1». Цей пристрій має довжину рубежу, що охороняється, до 200 м.

- «РИФ-РЛМ» відрізняється високими експлуатаційними характеристиками, стійкий у роботі. Приймач, передавач, стійка з телескопічним регулюванням, встановлена на бетонну основу і захищені метало рукавом джгути зручні для монтажу. В конструкції «РИФ-РЛ» використані кращі рішення його попередника - системи «ПРОТВА», рис.1.5.

- «ЕМЦ 200, 300, 500» відноситься до радіопроменевої системи виявлення порушників , принцип дії якої заснований на створенні в просторі між передавачем та приймачем електромагнітного поля, що формує об'ємну зону виявлення у вигляді витягнутого еліпсоїда обертання та реєстрації змін даного поля при перетинанні зони виявлення порушником.

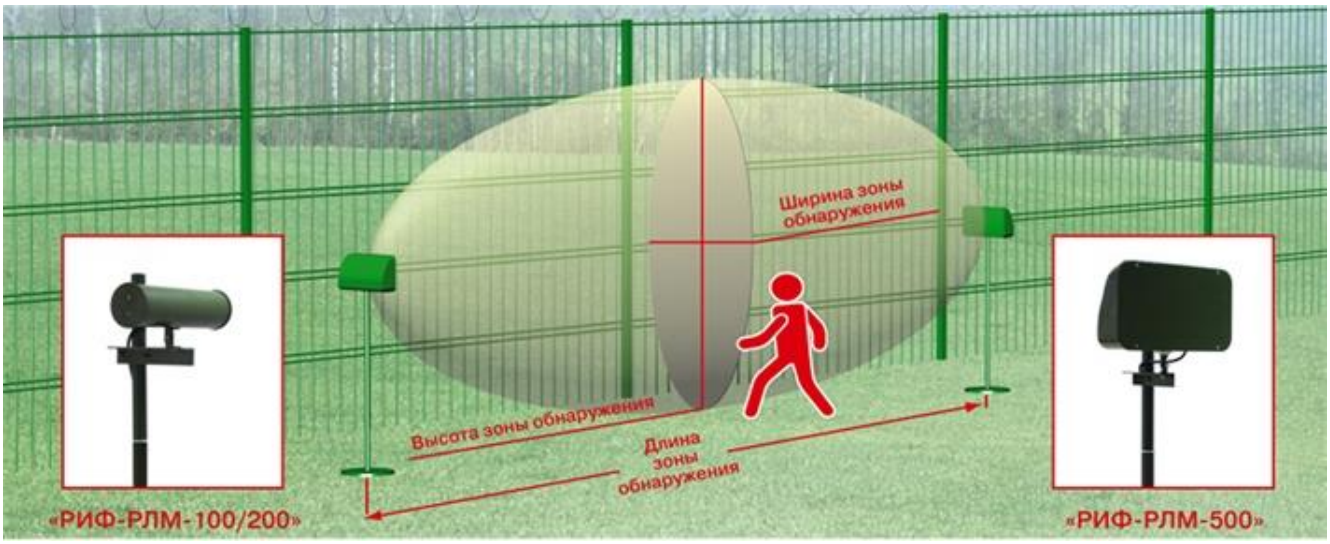


Рис.1.5. Двопозиційний радіопроменевій засіб виявлення. Схематичне зображення «РИФ-РЛМ»

Дальність дії радіопроменевої охоронної системи складає відповідно 200, 300, 500 метрів. Рекомендовано використовувати в якості третього рубежу охорони військових об’єктів, рис.1.6 та рис.1.7.

Рис. 1.6. Варіант розміщення радіопроменевої системи виявлення порушників «ЕМЦ 200, 300, 500»

Рис. 1.7. Варіант розміщення ЕМЦ системи по верху інженерного загородження

- «ГАРУС» відрізняється від наведених вище засобів виявлення відсутністю «мертвих зон» і малим споживанням електроенергії.

- «ЛЄНА-2» має невелику зону виявлення (діаметр не більше 1 м при довжині 125 м). Може використовуватися для прикриття вікон в будинках на нижніх поверхах, на інших окремих ділянках контуру, що охороняється.

- «ПРОТВА». Цей засіб виявлення доцільно застосовувати на периметрах, що мають чисельні вигини в азимутальній площині. Теоретично п’ять прийомо-передаючих пар дозволяють обладнувати одним сигналізатором ділянки спільною довжиною 500 м, а практично, з урахуванням перекриття ділянок, – 400 м. «ПРОТВА» може бути рекомендована для оснащення невеликих об’єктів (наприклад, чотири ділянки навколо складу-ангара плюс один біля в'їзних воріт).

- «РЛД-94». виготовляється в трьох модифікаціях із довжинами зон виявлення відповідно 30, 100 і 300 метрів. Його раціонально використовувати для захисту воріт, розривів в огородженні, що можуть утворювати, наприклад, під'їзні залізничні колії, водяні простори та ін.

Мікрохвильовий сповіщувач «АБРИС» (АП-200) призначений для застосування в системах охорони периметрів об’єктів і протяжних рубежів, рис.1.8. «АБРИС» упевнено виявляє подолання порушником зони, що охороняється, який рухається зі швидкістю від 0,1 до 7,0 м/с у повний зріст чи зігнувшись до висоти 0,7

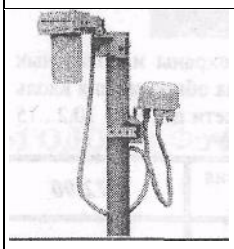
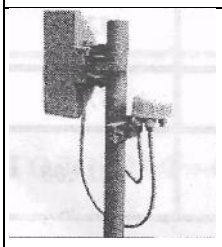
м і, по оцінці розробників, не реагує на дрібних тварин і птахів.

Рис.1.8. Двопозиційний мікрохвильовий сповіщувач «АБРИС»

Виріб «РЛД-94» виготовляється в трьох модифікаціях із довжинами зон виявлення відповідно 30, 100 і 300 м, див. таблиця 1.1. Його раціонально використовувати для захисту воріт, розривів в огородженні, що можуть утворювати, наприклад, під'їзні залізничні колії, водяні простори та ін. Модифікації на 100 і 300 м являють собою базовий комплект (передавач-приймач, розрахований на 30 м), дообладнаний спеціальними відбивачами.

Таблиця 1.1

Загальна характеристика «РЛД-94»

Зовнішній	Модель	Загальні відомості
	РЛД-94 УМ-050-18	Модель виробу призначена для застосування в приміщеннях і на коротких ділянках місцевості довжиною до 50 м. Передбачаються варіанти постачання з комплектом монтажних частин для установки виробу: на загородження, на стіні будинку; на металеву стійку; на асбоцементну трубу; на торцеву стіну коридору.
	РЛД-94 УМ-150-18	Модель виробу призначена для застосування на ділянках місцевості довжиною до 150 м. Передбачаються варіанти постачання з комплектом монтажних частин для установки виробу: на загородження, на стіні будинку; на металеву стійку; на спеціальних стійках виробу РЛД-73; на асбоцементну трубу.
	РЛД-94 УМ-300-18	Модель виробу призначена для застосування на ділянках місцевості довжиною до 300 м. Передбачаються варіанти постачання з комплектом монтажних частин для установки виробу: на загородження, на стіні будинку; на металеву стійку; на спеціальних стійках виробу РЛД-73; на асбоцементну трубу.

У радіохвильових системах чутливий елемент являє собою два паралельні провідники, один з яких приєднується до передавача, а другий – до приймача радіосигналу. Навколо такої пари формується зона виявлення. При появі в цій зоні людини або стороннього предмета подається сигнал тривоги. Такі системи можуть використовуватись для охорони як загороджених периметрів, так і відкритих територій. Найбільш поширені системи: «Промінь-М», «Газон», «Барьер-300/500», «FMW-3», «FMW-3T», «Піон-В».

Рис.1.9.Радіохвильовий сповіщувач «ПРОМІНЬ-М»

Система захисту периметру великої довжини (понад 5 км) будується на базі інтегрованого комплексу Багульник-М-УСО, рис.1.10.

Рис.1.10. Інтерфейс програмного модулю інтегрованого комплексу Багульник-М-УСО

До складу системи входять: 1-ий рубіж: сповіщувач провіднохвильовий Рельєф 1 призначений для охорони периметрів об'єктів, рис.1.11; датчик реєстрації подолання загороджень Багульник-М. Принцип дії заснований на створенні зони виявлення «козиркового» або «приземного» типів між двома ізольованими проводами, висотою до 1,8 м і довжиною до 250м. Зона виявлення точно повторює конфігурацію і рельєф рубежу охорони, що дозволяє ефективно використовувати сповіщувач на сильно пересіченій місцевості.

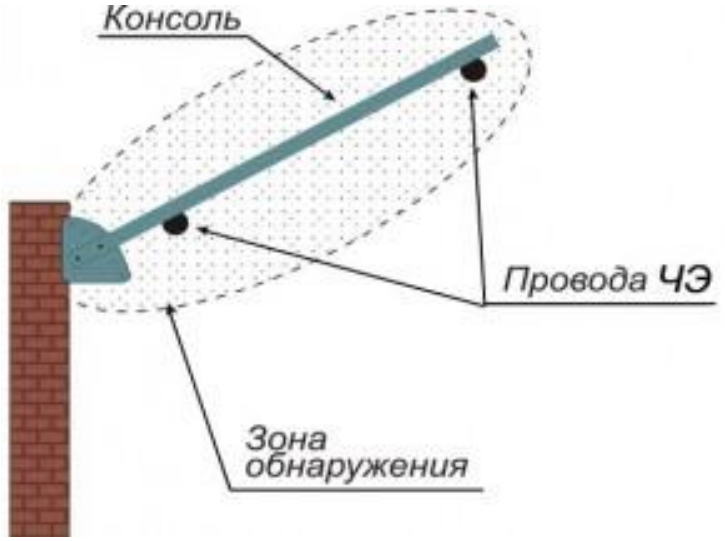


Рис.1.11.Сповіщувач провіднохвильовий Рельєф, встановлений по варіанту «козиркового» типу

2-ий рубіж: сповіщувач радіохвильовий Промінь-М. Діапазон робочих температур сповіщувача -40°…+50°С. У даному сповіщувачі закладена можливість – обмін інформацією з комп'ютеризованим пультом охорони по інтерфейсу RS-485.

1.2. Аналіз мобільних засобів охорони та особливості їх застосування

Досвід проведення антитерористичної операції на сході нашої країни, участі окремих підрозділів збройних сил України у миротворчих операціях, збройних конфліктах, проведення аналізу діяльності екстремістських організацій проти військових об’єктів показав, що ефективність підготовки військ (сил), збереження життя та здоров’я особового складу, охорона боєприпасів і військової техніки знаходяться у прямій залежності від якості організації охорони військових об’єктів,

а також можливості у автоматичному режимі виявляти порушників на підступах до об’єктів, що охороняються.

Обладнання радіоелектронними технічними засобами охорони (ТЗО) ближніх і дальніх підступів до позицій блокпостів, механізованих підрозділів, районів зосередження та розташування бойової техніки, складів дозволить вартам, патрулям, сторожовим постам, спостережним пунктам надійно охороняти військові об’єкти.

Аналіз останніх досліджень [11-13] з питань удосконалення систем технічного захисту військових об’єктів і підступів до них та їх порівняння із аналогічними системами збройних сил найбільш розвинених країн світу свідчить про те, що сучасні принципи організації системи охорони тимчасово розташованих військових об’єктів (ТРВО), що швидко розгортаються (ШвР), у ЗС України впроваджуються недостатньо ефективно.

В країнах НАТО (насамперед у збройних силах США) обладнання ТЗО ШвР почало розроблятися й застосовуватися ще з 70-х років минулого століття. У Радянському Союзі його розробка почалася в середині 80-х років. З утворенням незалежних держав цьому напрямку досліджень достатньої уваги не приділяється.

У 1972 році МО США ініціювало програму створення радіоелектронних засобів охорони (РЕЗО) баз і об’єктів BISS (Base and Installations Security System) для всіх видів ЗС. У програмі, що включала 50 окремих проектів, було покладено завдання розробки засобів охорони споруджень і внутрішніх приміщень, де зберігалася зброя й боєприпаси, а також окрема програма створення автономних і дистанційно керованих розвідувально-сигналізаційних систем поля бою.

З 1985 року почалися конструкторські розробки та технічна реалізація програми впровадження автономної системи РЕЗО військових баз і об’єктів TASS (Tactical Autonomous Security System) [11-13].

Для побудови мереж ТЗО ШвР мобільних об’єктів (літаків, бойової техніки, транспортних засобів) на тимчасових стоянках, а також окремих будинків, внутрішніх приміщеннях складів, ангарів і захищених укриттів застосовуються переносні засоби охорони об’єктів.

Найбільш широкого використання в охороні тимчасових і рухливих об’єктів ЗС США одержали переносні РЛС AN/ PPS-5 і -15 різних модифікацій, рис.1.12. Патрулі охорони озброюються ручними РЛС (AN/PPS-9, -11, -12, -13, -14).

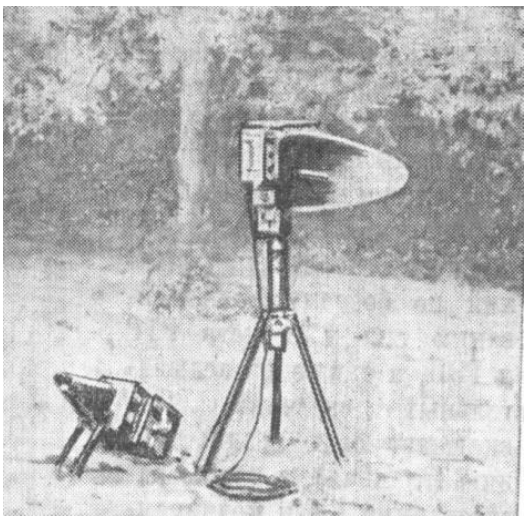


Рис.1.12. РЛС AN/ PPS-5

Для охорони тактичних підрозділів сухопутних військ США розроблена легка портативна РЛС OGR (Organic Ground moving target indication Radar), що забезпечує виявлення людей, що рухаються, і транспортних засобів на дальності до 10…20 км в простих і складних метеоумовах. Цю станцію розміщують на автомобілі, що дозволяє організовувати мобільну охорону замість використання для цих цілей переносних РЛСП, протипіхотних і сигнальнобойових мін. Також використовується переносна тактична система охорони OSTSS (Omnisense Tactical Security System), рис.1.13, з мініатюрними радіостанціями охорони TSR (Tactical Sentry Radio) та акустична РСП ACVS (Acoustic Cueing and Validation Sensor), що виявляє й класифікує цілі на дальності від 20 до 40 км [11-13].

Рис. 1.13. Переносна тактична система охорони OSTSS

При необхідності швидкого створення системи охорони тимчасових споруджень і мобільних об’єктів широко застосовуються розвідувально-сигналізаційні системи. Для цих цілей на сьогодні використовуються системи IREMBASS, PEWS-2, MIDS-EMIDS, REMBASS-2, TRESS, MPNSS та ін. [11-13], рис. 1.14.

Рис.1.14. Розвідувально-сигналізаційна система REMBAS

Для організації охорони ТРВО можливе впровадження двох груп ТЗО – відповідно рубіжно-сигналізаційних (як правило активних) та розвідувально-сигналізаційних (в основному пасивних), хоча в деяких випадках ТЗО можуть використовуватися подвійно. У перших – порушник виявляється по його взаємодії зі спеціально сформованим електромагнітним полем; внаслідок цього відсутнє радіомаскування, споживається підвищена потужність електроживлення, однак вони дозволяють контролювати велику територію на ближніх і дальніх підступах.

Другі – виявляють порушника по внесеним ним змінами в існуюче фізичне поле (магнітне, теплове, вібраційне) володіють радіо- і, як правило, візуальною маскованістю (встановлюються в ґрунт, вбудовуються в місцеві предмети).

У рубіжно-сигналізаційній системі для охорони ТРВО сигнал тривоги повинен подаватися автоматично. В розвідувально-сигналізаційній системі охорони рішення про ідентифікацію події виявлення (порушник/перешкода) приймає, як правило, оператор, що перебуває біля головного або переносного пульта керування й індикації (ПКІ).

Системи, що швидко розгортаються для охорони ТРВО, повинні бути розраховані на тимчасову (від декількох дів до 2...3 місяців) охорону об’єктів, блокуючи окремі рубежі (райони) й підступи до них, після чого складові частини комплексу охорони згортаються й розгортаються (розставляються) в іншому місці.

Пост охорони, на якому розташовується головний ПКІ, може бути стаціонарним або мобільним (переносним або розташовуватися на автомобілі). Передача інформації на ПКІ повинна здійснюватися переважно за допомогою ультракороткохвильових (УКХ) радіоканалів в діапазоні 700-900 МГц, у тому числі з використанням ретрансляторів. При цьому системи охорони можуть комплектуватися декількома переносними ПКІ, це забезпечує тактичну гнучкість застосування на місцевості та резервування при відмові (знищенні) одного з них. Працездатність ТЗО перевіряється прямим (в автоматичному режимі) викликом по радіоканалу на періодичний самоконтроль.

Як правило, датчики виявлення засобів ТЗО ШвР є точковими, зона виявлення повинна бути секторною або круговою контролюючи площу в радіусі до 300 м. Такі засоби, як правило, маскуються на фоні предметів, що їх оточують. Дія засобів виявлення заснована на відомих фізичних принципах з використанням радіолокаційного, телевізійного (ТВ), інфрачервоного (ІЧ), тепловізійного (ТпВ), фотоелементного, лазерного, магнітного, електромагнітного, сейсмічного, вібраційного принципів виявлення, широко використовуються електронно-оптичні прилади, а також різні комбінації цих пристроїв, РЛСП станцій виявлення й спостереження [11].

До основних технічних характеристик ТЗО відносяться: дальність виявлення, точність виявлення параметрів руху об’єкта, завадозахищеність передачі інформації прямого та зворотного каналів, час пошуку, дальність та швидкість передачі інформації, масо-габаритні показники, вартість, надійність функціонування, економічність, прихованість, криптографічний захист від несанкціонованого доступу в радіоканалі, потужність енергоспоживання [11].

Джерелами хибних тривог у ТЗО систем ШвР можуть бути тварини, сильний вітер у поєднанні із близько розташованою рослинністю, блискавки при грозі,

опади. Всі засоби, за винятком інфрачервоних (сильний туман), є всепогодними, але існують обмеження на їхнє застосування в умовах високого сніжного покрову, трави, кущів, дерев, гірських перевалів та населених пунктів.

Основним завданням ТЗО для охорони ТРВО повинна бути тимчасова, швидка й надійна організація охорони районів, рубежів, об'єктів, місць дислокації особового складу, бойової техніки, арсеналів зі зброєю, складів, сигналізуючи про вторгнення порушників, диверсантів, злодіїв. Рубежі охорони об'єктів, що охороняються, повинні бути замкнуті, зони виявлення – перекриватися, але на місцевості зі складним, горбкуватим ландшафтом, з лісами та ярами цю вимогу можливо реалізувати тільки частково.

Тому в таких районах додатково необхідно використовувати РЛСП і РЛСР наземних цілей, у схованках біля стежок лісових доріг, а в ярах, на гірських перевалах слід закладати дистанційно керовані радіоелектронні (оптичні) засоби виявлення. Такі радіоелектронні системи ТЗО дозволятимуть непомітно виявляти, підраховувати, класифікувати й визначати напрямок пересування живої сили й самохідної техніки, передавати дані на ПКІ по радіоканалу. Передача інформації (сигналів виявлення) від таких ТЗО на ПКІ (віддалених на 10…20 км) повинна здійснюватися по завадозахищеним УКХ радіоканалам.

Радіоелектронне обладнання ТЗО повинно живитися від різних джерел електроживлення в основному від автономного живлення: від батарей, акумуляторних батарей (АКБ) і сонячних батарей. Такі батареї обов'язково повинні підзаряджати АКБ, забезпечувати 30…50 Вт потужності, що достатньо для роботи апаратури ТЗО. При цьому повинно передбачатися й живлення від зовнішньої електромережі та електрообладнання автомобілів.

Сумісне використання ТЗО ШвР і засобів виявлення РЛСП дозволяє вирішувати декілька завдань: здійснювати малопомітне тимчасове сигналізаційне сканування (блокування) ділянки периметра об'єкта, виявляти порушників, що перетинають рубіж; вести приховану інженерно-технічну розвідку на неконтрольованій території (у тому числі під час бойових дій) в місцях ймовірного

пересування озброєних людей, транспорту, бойової техніки, сигналізуючи про їхню появу, чисельність та напрямок руху.

ТЗО які призначені для охорони ТРВО можуть також використовуватися в системах охорони стаціонарних об’єктів та великих приміщень (ангарів, складів). Радіоелектронні засоби ТЗО доцільно також використовувати при виконанні задач по охороні державного кордону підрозділами Державної прикордонної служби, службами МНС в літній період у важкодоступних районах найбільш вірогідного загорання лісів, при слідкуванні за браконьєрами на річках та озерах (особливо в ночі), незаконним мисливством.

Для охорони військових об’єктів ЗС України необхідно розробляти та використовувати уніфіковані, блочно-модульні охоронні системи з розширеними охоронними функціями, які вирішують задачі розвідки, виявлення, сигналізації та класифікації порушення (порушників). Вони повинні представляти собою інтегровані охоронні комплекси, що володіють широкими можливостями (дистанційне керування, позиціонування на місцевості, GSM, супутниковий зв’язок, цифрову передачу даних та ін.).

Додаткове використання можливостей комп’ютерної техніки на ПКІ дозволить виконувати тривимірне відображення місцевості із заданої точки місцезнаходження спостерігача або віртуальний обліт місцевості з обстановкою, яка нанесена з врахуванням сигналів (інформації), що передають в автоматичному режимі кінцеві пристрої ТЗО. Це дає можливість на головному ПКІ приймати рішення з адекватного реагування на ситуацію, що складається.

1.3. Аналіз методів ідентифікації особи

В ТЗО ШвР постає питання ідентифікації особи при перетині границі захисту. Аналіз робіт [1, 4, 6-10] показав, що можна виділити три найпоширеніших види ідентифікації:

1. Парольна ідентифікація. Ще не дуже давно парольна ідентифікація була чи ледве не єдиним способом визначення особистості користувача. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні.

Недоліком парольної ідентифікації є значна залежність надійності ідентифікації від користувачів, точніше від обраних ними паролів. В нашому випадку, при побудові ТЗО ШвР використання парольної ідентифікації вимагає встановлення додаткових засобів зчитування, затрат часу на введення паролю та буде досить незручним у використанні.

2. Апаратна ідентифікація. Цей принцип ідентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем, що перебуває в його ексклюзивному користуванні. Мова йде про спеціальні електронні ключі.

На даний момент найбільше поширення одержали два типи пристроїв. До першого відносяться всілякі карти. Найбільш надійними вважаються смарт-карти - аналоги звичних багатьом людям банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом і т.д. (рис. 1.15).

Рис. 1.15. Картки для ідентифікації співробітників

Іншим типом ключів, які можуть використатися для апаратної ідентифікації, є так звані токени (рис. 1.16). Ці пристрої мають власну захищену пам’ять і підключаються безпосередньо до портів USB, LPT турнікетні пристроїв. Головною перевагою застосування апаратної ідентифікації є досить висока надійність. В будований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції.

Рис.1.16. Вигляд токенів

Недоліком апаратної ідентифікації є висока ціна. Взагалі ж останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте для введення в експлуатацію системи майнової ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися або можуть бути загублені користувачами. При побудові ТЗО ШвР досить важко реалізуються за рахунок використання систем у польових умовах.

3. Біометрична ідентифікація. Біометрія – це ідентифікація людини за унікальними, властивими тільки їй біологічними ознаками. Сьогодні експлуатується вже більше десятка різних біометричних ознак. Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів (рис. 1.17). Так що користувачам, що вирішили використати біометричну ідентифікацію, є із чого вибрати.

Рис.1.17. Дактилоскопічний сканер

Розпізнавання по відбитку пальців є найпоширенішим статичним методом біометричної ідентифікації, в основі якого лежить унікальність для кожної людини малюнка папілярних візерунків на пальцях. Папілярні відбитки посідають перше місце серед біометричних характеристик людини через те, що вони не змінюються протягом всього життя. Вважається, що ймовірність збігу відбитків пальців рук однієї людини з іншою становить 1 до 64 млрд. [4, 6-10]. Це означає, що такий збіг відбитків на всій Земній кулі просто неможливий. Тому папілярні відбитки можуть бути основою для сучасних і перспективних біометричних систем охорони об'єктів.

Основним недоліком біометричної ідентифікації є вартість устаткування та незручність використання для тимчасової охорони периметру. В загальному випадку перелік ідентифікаторів, що можуть використовуватися на об’єктах охорони наведений на рис. 1.18.

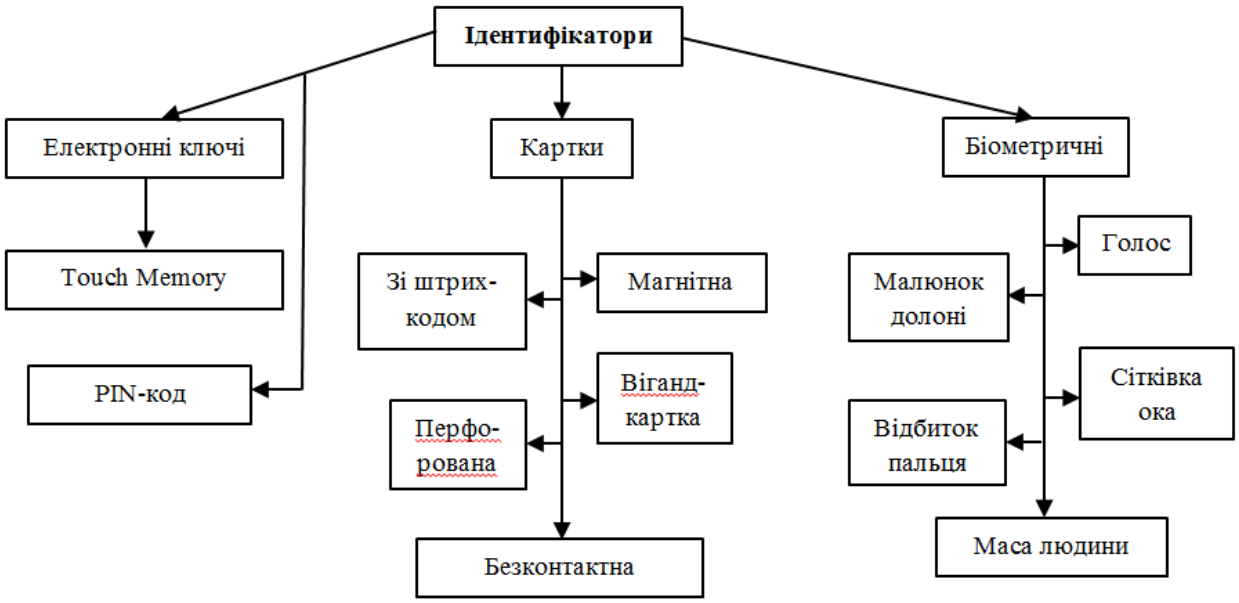


Рис.1.18. Класифікація ідентифікаторів

Поступово все більшого поширення одержує багатофакторна ідентифікація, коли для визначення особистості застосовується відразу кілька параметрів. Причому комбінуватися ці фактори можуть у довільному порядку, рис.1.19.

Рис.1.19. Пристрій для багатофакторної ідентифікації

На даний момент існує досить багато методів біометричної ідентифікації, які діляться на дві групи – статичні й динамічні методи [1, 4-10]. Статичні методи біометричної ідентифікації ґрунтуються на фізіологічній (статичній) характеристиці людини, тобто унікальній характеристиці, даної йому від н

Загальною характеристикою для порівняння різних методів і способів біометричної ідентифікації – є статистичні показники – помилка першого роду (не пустити в систему «свого») і помилка другого роду (пустити в систему чужого).

Дуже цікавою пропозицією американських учених для ідентифікації особи виступає метод імплантації чіпів. Про впровадження й апробацію даної технології пише Ківі Берн в опублікованій статті: «На безпрецедентний крок наважилися працівники прокуратури Мексики. Генеральний прокурор країни Рафаель Маседо де ла Конча (Rafael Macedo de la Concha) і 160 його підлеглих імплантували собі під шкіру мікрокапсули ідентифікації VeriChip (розробка американської компанії Applied Digital Solutions, Флорида).

Як відомо, такого роду RFID-чіпи вже досить широко використовуються для мітки худоби й свійських тварин, однак добровільна імплантація капсул VeriChip людьми – справа усе ще вкрай рідке. Наразі триває масова «чіпізація» держслужбовців у країнах, де триває нестабільна політична обстановка, яка обтяжується викраденням людей, шантажем, рис.1.20.

Що стосується визначення місця розташування людини з RFID-чипом, то та сама фірма-виробник Applied Digital Solutions визнає, що поки подібна технологія

перебуває лише в стадії розробки, та й то має потребу в зовнішньому GPS-пристрої розміром приблизно з кардіостимулятор.

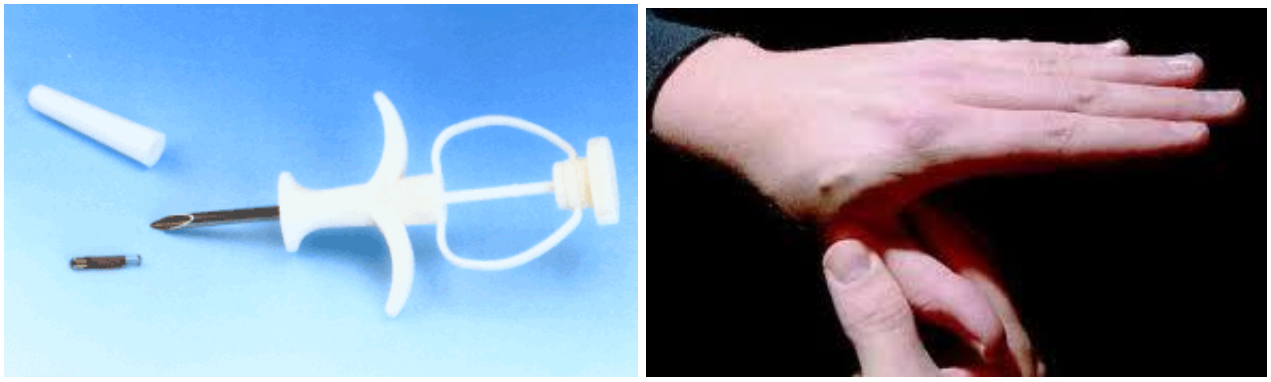


Рис. 1.20. Вигляд пристроїв для імплантації чіпів та людина після загоєння з чіпом в руці

І поки VeriChip визначиться сканером-считувачем на відстані не більше 3-4 метрів, рис.1.21. Крім того, злочинці, що спеціалізуються на викраденні людей, перш за все ретельно обстежують викраденого на предмет присутності імплантованого чіпа.

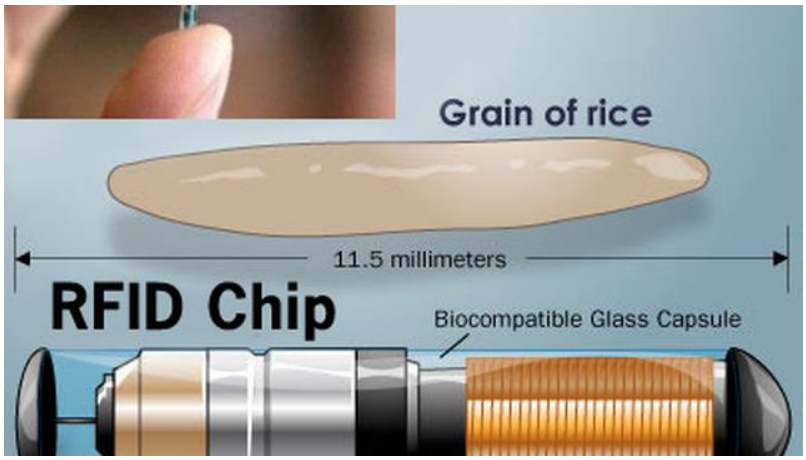


Рис. 1.21. Вигляд RFID-чіпу

RFID-чіпи з можливостями шифрування є цілком адекватним засобом аутентифікації й використовуються в перепустках урядових закладів і деяких корпорацій, рис.1.22.

Рис.1.22.Вигляд перепустки з використанням RFID-технології

На сьогоднішній день фірма Applied Digital Solutions – це єдине місце, де займаються підшкірними ін'єкціями RFID-мікросхеми VeriChip не тільки тваринам, але й людям (gvsregistry.4verichip.com). Глава ADS Скот Сильвермен (Scott Silverman) виступив на конгресі ID World, повідомивши, що його фірма готується до запуску в найближчому майбутньому спеціального сервісу VeriPay, що дозволить людям розплачуватися за товари й послуги за допомогою чіпа, імплантованого в руку.

Одним з головних факторів, які діють на роботу систем охорони, є навколишнє середовище. Тому надійність роботи всіх складових системи охорони багато в чому визначається тим, яким чином її компоненти, а також їхнє функціонування здатні врахувати зміну параметрів навколишнього середовища й адаптуватися до них. Впровадження RFID-чіпів в постійні перепустки є досить ефективним засобом для ідентифікації в зоні контрольно-пропускного пункту.

Це дозволить нам зменшити час на ідентифікацію постійних працівників та підвищить зручність використання таких перепусток за рахунок безконтактної ідентифікації на відстані до 200 метрів. При цьому доставати та пред’являти перепустку буде не обов’язково.

1.4. Аналіз проблеми забезпечення кібербезпеки компонентів IoT систем

У червні 2018 року компанія Juniper Research у дослідженні ринку інтернету речей спрогнозувала зростання вдвічі кількості таких пристроїв до 2022 року. Якщо зараз аналітики оцінюють число активних IoT-пристроїв у 21 мільярд, то через чотири роки їх кількість перевищить 50 мільярдів. У зв'язку з розвитком IoT-технологій висловлюють занепокоєння фахівці у сфері інформаційної безпеки [14-18]. На їхню думку, величезна кількість погано захищених інтернет-девайсів дає нові можливості кіберзлочинцям, яким уже вдалося зламати ряд IoT-систем. Особливо актуально дана задача ставиться при використанні даних засобів на об'єктах критичної інфраструктури.

Гучна кібератака трапилася в жовтні 2016 року, коли недоступним виявився ряд популярних ресурсів, сервісів і соціальних мереж: Amazon, Pinterest, Twitter, Soundcloud, Spotify, Reddit, GitHub, Starbucks, CNN, The New York Time та ін. Через атаки постраждали власники сайтів, які працюють на серверах компанії Dyn. Відомо, що зловмисники використовували програму Mirai, здатну знаходити в мережі незахищені пристрої інтернету речей, такі, як роутери, камери стеження, цифрові відеомагнітофони і т.д. У ботнет, згідно з даними Dyn, були об'єднані понад 100 000 незахищених підключених пристроїв, оскільки працювали без захисту паролів. Робота атакованих сайтів була відновлена лише через 14 годин.

Актуальність проблеми підкреслюється інцидентами, втрати капіталу від яких вимірюються мільярдами доларів: Industroyer, BrickerBot, Mirai – і це лише видима верхівка айсберга. Дані досліджень корпорації HP, метою яких було не виявити якісь конкретні небезпечні інтернет-пристрої і викрити їх виробників, але позначити проблему ІБ-ризиків в світі IoT в цілому, звертають увагу на проблеми як з боку власників пристроїв, так і на проблеми, над усуненням яких повинні працювати розробники. Так, на самому початку експлуатації користувачеві обов'язково потрібно замінити фабричний пароль, встановлений за замовчуванням, на свій особистий, оскільки фабричні паролі однакові на всіх пристроях і не відрізняються стійкістю. Оскільки не всі прилади мають вбудовані засоби ІБ-захисту, власникам також слід подбати про встановлення зовнішнього захисту,

призначеного для домашнього використання, щоб інтернет-пристрої не стали відкритими шлюзами в домашню мережу або прямими інструментами заподіяння шкоди.

У ході проведеного HP дослідження виявлено, що приблизно в 70% проаналізованих пристроїв не шифрується бездротовий трафік. Веб-інтрефейс 60% пристроїв експерти HP вважають небезпечним через недосконалу організацію доступу і високий ризик міжсайтового скриптингу. У більшості пристроїв передбачені паролі недостатньої стійкості. Приблизно 90% пристроїв збирають ту чи іншу персональну інформацію про власника без його відома. Всього ж фахівці HP нарахували близько 25 різних вразливостей у кожному з досліджених пристроїв і їх мобільних та хмарних компонентах. Висновок експертів HP невтішний: безпечної системи IoT сьогодні не існує. Особлива небезпека для інтернету речей прихована в контексті поширення цільових атак (APT). Варто тільки зловмисникам проявити інтерес до будь-кого, і наші помічники зі світу IoT перетворюються на зрадників, нарозхрист відкривають доступ у світ своїх власників.

Були виділені такі слабкі місця IoT [2]: перехід на IPv6; живлення датчиків; стандартизація архітектури і протоколів, сертифікація пристроїв; інформаційна безпека; стандартні облікові записи від виробника, слабка аутентифікація; відсутність підтримки з боку виробника для усунення вразливостей; важко або неможливо оновити ПЗ і ОС; використання текстових протоколів і непотрібних відкритих портів; використовуючи слабкість одного гаджета, хакеру легко потрапити в усю мережу; використання незахищених мобільних технологій; використання незахищеної хмарної інфраструктури; використання небезпечного ПЗ. Оскільки питання стоїть надзвичайно гостро, компанії-розробники техніки, засобів комунікації, мережних пристроїв, програмного забезпечення, кіберзахисні компанії переймаються пошуками засобів захисту пристроїв IoT. Однією з провідних компаній у розробці засобів безпеки в IoT є Cisco Systems, яка відіграла провідну роль у розробці моделі IoT на Всесвітньому форумі IoT (IWF), розробила фреймворк безпеки IoT, що став корисним доповненням до еталонної моделі. На

рисунку 1 продемостроване середовище безпеки, пов’язане з логічною структурою IoT.

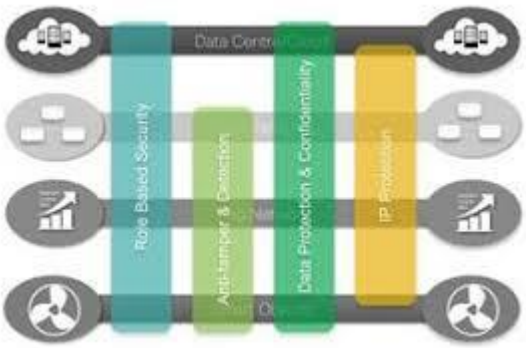


Рис.1.23. Середовище безпеки IoT

Модель Cisco IoT є спрощеною версією моделі Всесвітнього форуму IoT. Вона складається з наступних рівнів:

1. «Розумні» об’єкти та вбудовані системи: ця частина IoT найбільш вразлива.

2. Туманна, периферійна мережа: цей рівень включає дротові та бездротові з’єднання пристроїв IoT. Ключовою проблемою є велика варіативність мережевих технологій і протоколів, що використовується різними використовуваних різними пристроями IoT, і необхідність вироблення і втілення єдиної політики безпеки.

3. Ядро мережі: рівень ядра мережі надає шляхи для передачі даних між платформами в центрі мережі і пристроями IoT. Тут проблеми безпеки ті ж, що в традиційних мережах. Однак величезна кількість кінцевих вузлів, з якими треба взаємодіяти і управляти ними, створює значну проблему для безпеки.

4. Центр даних та хмарні сервіси: цей рівень містить платформи для додатків, зберігання даних і управління мережею. IoT не додає на цей рівень ніяких нових проблем безпеки, крім необхідності мати справу з величезною кількістю окремих кінцевих вузлів.

За допомогою цієї чотирьохрівневої архітектури модель Cisco визначає чотири загальних можливості безпеки, що охоплюють кілька рівнів:

1. Безпека на основі ролей: системи управління доступом на основі ролей призначають права доступу ролям, а не окремим користувачам. Користувачам, в свою чергу, зіставляються різні ролі, або статично, або динамічно, відповідно обов’язків.

2. Захист від втручання і виявлення втручань: ця функція особливо важлива на рівні пристроїв і туманної мережі, але поширюється також і на рівень ядра мережі. Всі ці рівні можуть використовувати компоненти, що фізично знаходяться на території вільного доступу до них будь-ким.

3. Захист даних і конфіденційність: ці функції охоплюють всі рівн архітектури.

4. Захист протоколів інтернету: захист «даних в русі» від прослуховування і перехоплення важливий для всіх рівнів.

На рисунку 1 відзначені конкретні функціональні області безпеки поверх чотирьох рівнів моделі IoT. У документі Cisco також пропонується концепція безпеки IoT, що визначає компоненти функції безпеки для IoT, яка охоплює всі рівні:

1. Аутентифікація: цей компонент охоплює елементи, які ініціюють доступ, і в першу чергу ідентифікує пристрої IoT. На відміну від типових корпоративних мережевих пристроїв, кінцеві пристрої IoT повинні оснащуватися такими методами аутентифікації, які не вимагають втручання людини. До таких методів належать радіочастотні мітки, сертифікати x.509 або MAC-адреси кінцевих пристроїв.

2. Авторизація: авторизація управляє доступом до пристрою через структуру мережі. Цей елемент включає в себе контроль доступу. Разом з рівнем аутентифікації він виробляє необхідні параметри для того, щоб дозволити обмін інформацією між пристроями та між пристроями і прикладними платформами, тим самим забезпечуючи роботу IoT-служб.

3. Мережева політика: цей компонент охоплює всі елементи, які здійснюють маршрутизацію і транспортування трафіку з кінцевих пристроїв інфраструктурою, будь то контроль, управління або власне трафік даних.

4. Аналітика безпеки: цей компонент включає всі функції, необхідні для централізованого управління пристроями IoT. На основі видимості виникає здатність здійснювати контроль, включаючи конфігурацію, патчі і оновлення, а також контрзаходи для припинення загроз.

У процесі дослідження розробляється комплекс заходів та засобів підвищення безпеки для IoT. Багато компаній на сьогодні представили свої моделі захисту, які

постійно намагаються стандартизувати, співвіднести та впровадити. Дослідження технологій та засобів безпеки в IoT, пошук оптимальних моделей безпеки в усіх рівнях: апаратної частини, програмної частини, рівні користувача є надважливим завданням сьогодення.

Висновки до першого розділу

1. В результаті проведеного аналізу фізичних принципів дії засобів виявлення, що використовуються в системах охорони периметру, визначено переваги та недоліки кожного з них, представлено класифікацію систем охорони периметру та класифікацію периметрових засобів виявлення, розглянуті основні типи загороджувальних конструкцій та найбільш відомі системи охорони периметру.

2. Аналіз мобільних засобів охорони дозволив визначити склад, функціональні особливості такого роду систем. Визначено, що для організації охорони тимчасово розташованих об’єктів можливе впровадження двох груп технічних засобів охорони – відповідно рубіжно-сигналізаційних та розвідувально-сигналізаційних.

3. Проведений аналіз методів ідентифікації особи дозволив визначити, що найбільш вживаними є парольна ідентифікація, апаратна ідентифікація та біометрична ідентифікація.

4. Визначено, що для проведення процедури ідентифікації особи у швидкорозгортаючих системах охорони периметру необхідним є використання RFID-технологій.

5. Проведено аналіз проблем забезпечення кібербезпеки компонентів IoT систем дозволив визначити слабкі сторони IoT, досліджено рівні моделі Cisco IoT.

6. Встановлено, що з метою підвищення рівня захищеності необхідним є удосконалення існуючих моделей та методів побудови швидкорозгортаючих систем охорони периметру шляхом інтеграції переваг вибраних засобів та технологій в єдину систему.

2. МОДЕЛЮВАННЯ IoT СИСТЕМИ ОХОРОНИ ПЕРИМЕТРУ

2.1. Структурна модель IoT системи охорони периметру

Проведемо розробку моделі системи охорони периметру, що являє собою IoT систему, спрямовану на підвищення рівня захищеності (периметрового захисту) об'єкту охорони, шляхом автоматизації процесу виявлення порушників периметру, прийняття управлінських рішень щодо генерації тривоги по підрозділу. Дана модель у подальшому буде використана як базова для розробки технології забезпечення кібербезпеки її компонентів.

Поставлена мета досягається синтезом інтегрованих блоків, а саме впровадженням: підсистеми безконтактної радіочастотної ідентифікації (RFID) (Модуль 1); підсистеми інтелектуального відеоспостереження (Модуль 2); СППР із виявлення та попередження НСД на території об'єкту охорони (Модуль 3); підсистеми виявлення руху по контуру периметру захисту (Модуль 4). Структурна схема складових IoT системи представлена на рис. 2.1 [3].

Основними задачами Модулю 1 (М1) є:

– ідентифікація персоналу на території об'єкту охорони;

– визначення місцезнаходження персоналу на території об'єкту охорони;

– визначення персоналу, що наближається до периметру території об'єкту охорони.

Вихідними даними цього модулю є цифрова комбінація ідентифікатора, яка слугує вхідним потоком для роботи Модулю 3.

До основних задач Модулю 2 (М2) належать:

– ведення відеоспостереження за персоналом на території об'єкту охорони;

– ведення відеоспостереження за периметром території об'єкту охорони;

– надання користувачу інформації про порушника, який потрапив на територію об'єкту охорони;

– передача відеоінформації про НСД користувачу для оперативного прийняття адекватного рішення.

Основними задачами Модулю 3 (М3) є автоматизація процесів прийняття управлінських рішень оператором з:

–виявлення суб'єктів погроз;

– категоризації суб'єктів погроз за принципом небезпечності;

– визначення категорії небезпеки.

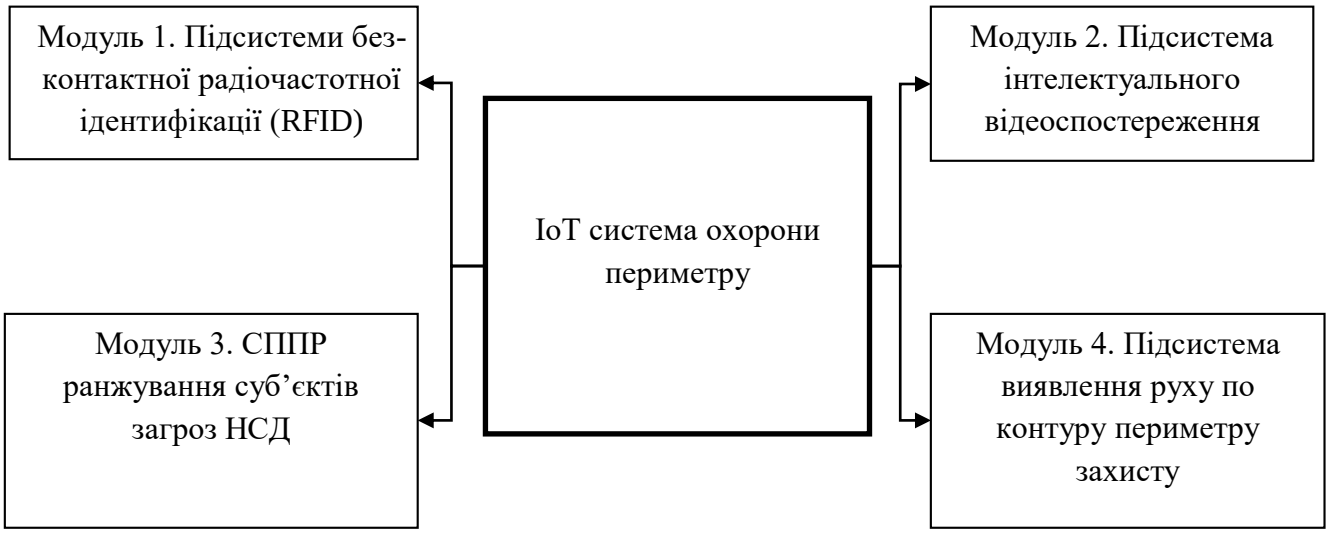


Рис. 2.1. Структурна схема IoT системи охорони периметру

Основною задачею Модулю 4 (М4) є виявлення вторгнення на територію периметру об'єкту охорони.

Модель взаємодії компонентів системи представлена на рис. 2.2. Вхідними даними системи є $\mathbf{F}=\{F_1,\ldots,Fi\}$ – множина сигналів RFID-міток, що отримані RFID-зчитувачами, $\mathbf{G}=\{G_1,\ldots,G_k\}$ – потік відеоданих, що надходить із відеокамер, $\mathbf{R_{інф}}=\{R_{інф1},\ldots,R_{інфр}\}$ – потік інформації, що надходить від ресурсів захисту території, $\mathbf{H}=\{H_1 \ldots H_y\}$ – множина сигналів від датчиків руху.

Інформаційні потоки для взаємодії системи складають:

– F_{ikod} – цифровий код (ідентифікатор), отриманий від RFID-мітки i-го працівника, $i=\overline{1\ldots n}$;

– $\mathbf{G_v}=\{G_{v1},\ldots,G_{vn}\}$ – послідовність оцифрованих кадрів у вигляді зображень у форматі BMP, що надходять від відеокамер;

– $\mathbf{P}=\{P1,\ldots,P\eta\}$ – виявлені суб'єкти погроз;

– **W**=*{W₁,…,Wλ}* – множина параметрів, що контролюються та аналізуються для визначення категорії небезпеки суб'єктів погроз.

Керуючими впливами виступають: F_{ikodz} – ідентифікатор *i*-ої особи персоналу.

Вихідним параметром системи є інформативний вектор **W***=*{Wi}*, i=1…λ, який передається каналами зв'язку як електронне повідомлення добового наряду об'єкту охорони, і, у разі потреби, до зовнішніх силових структур; інформаційний вектор **D**=*{Dl}*, *l=1…ε*, генерується системою автоматично та видається черговому добового підрозділу, передається у разі потреби, до зовнішніх силових структур; **R** – рішення СППР із ранжування суб'єктів загроз на території об'єкту охорони, **S** – рішення СППР із виявлення НСД суб'єктів загроз на території об'єкту охорони.

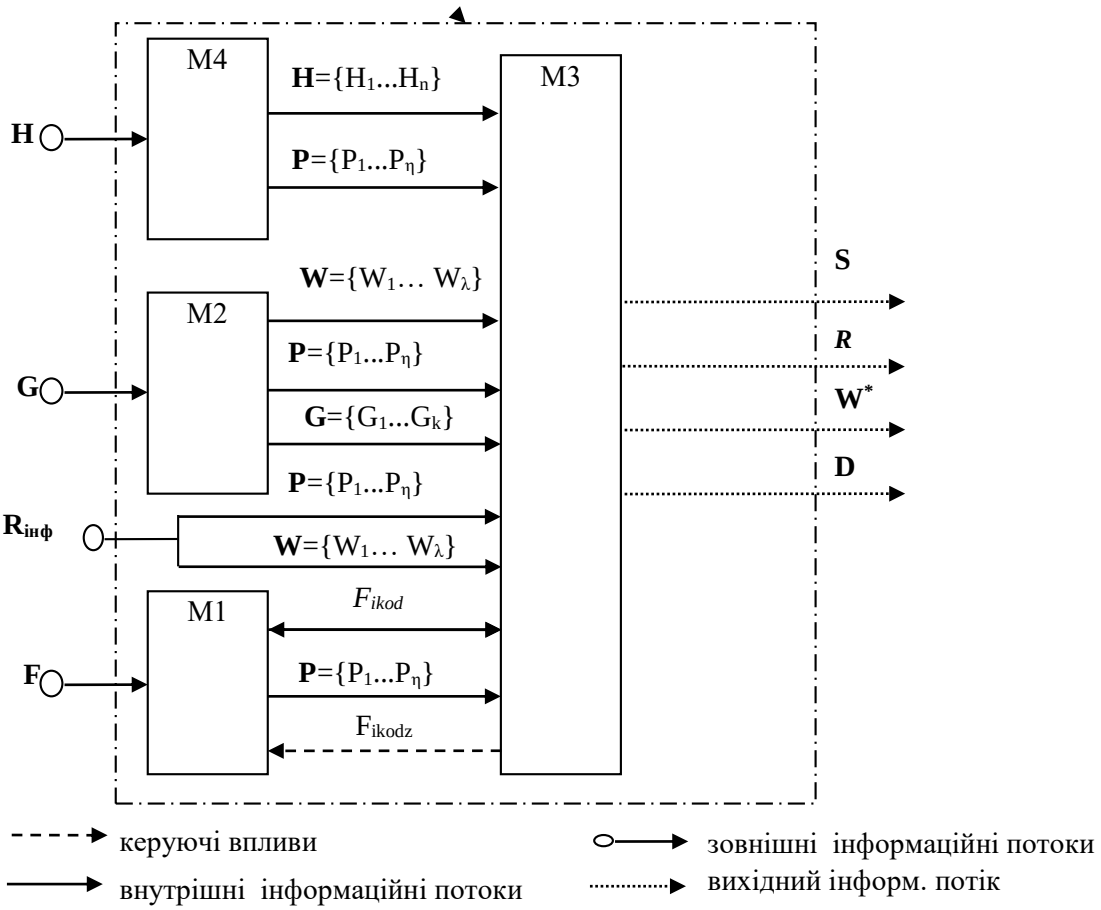


Рис. 2.2. Модель взаємодії компонентів IoT системи охорони периметру

Проведемо побудову моделі прояву суб'єктів погроз виникнення НСД. До суб'єктів погроз (Р) відносимо: психічно неврівноважених осіб (P_1); шпигунів (P_2); регіональні терористичні організації (P_3); міжнародні терористичні організації (P_4); екстремістів-одинаків або групи екстремістів (P_5); диверсійно-розвідувальні групи (P_6). Їх можна представити у вигляді відкритого класифікаційного угрупування суб'єктів погроз $\mathbf{P} = \bigcup_{\eta} P_{\eta}$ (множини суб'єктів погроз), які відповідно до умов експлуатації системи можна доповнювати або адаптувати.

Далі необхідно розробити, модель прояву суб'єктів погроз виникнення НСД на території об'єкту охорони, модель процесу визначення рівня небезпеки суб'єктів погроз виникнення НС на території об'єкту охорони, блок прийняття управлінських рішень.

2.2. Модель прояву порушників на території об'єкту охорони

Аналіз функціонування об'єктів охорони виявив потенційні об'єкти ураження, можливість проведення терористичних актів або інших дій на яких матиме максимальний вражаючий вплив. До таких об'єктів пропонується віднести: вантаж, особа (об'єкт охорони) (X_1^p); інформація (X_2^p); техніка підрозділу служби охорони (X_3^p); вузол зв'язку (X_4^p); зброя підрозділу служби охорони (X_5^p); довольче забезпечення (X_6^p). До персоналу на який може здійснюватися напад пропонується віднести: старший позиції (N_1^l); черговий зміни (N_2^l); оператор посту (N_3^l); зв'язківець (N_4^l); медик (N_5^l); чатовий (N_6^l). Аналогічним чином, отримуємо наступні відкриті класифікаційні угрупування:

$\mathbf{N} = \bigcup_{j} N_j$ – множина персоналу, на який може бути здійснено напад як наслідок НСД;

$\mathbf{X} = \bigcup_{a} X_a$ – множина об'єктів ураження, на які здійснюється напад.

Модель прояву порушників на території об’єкту охорони представлено на рис. 2.3.

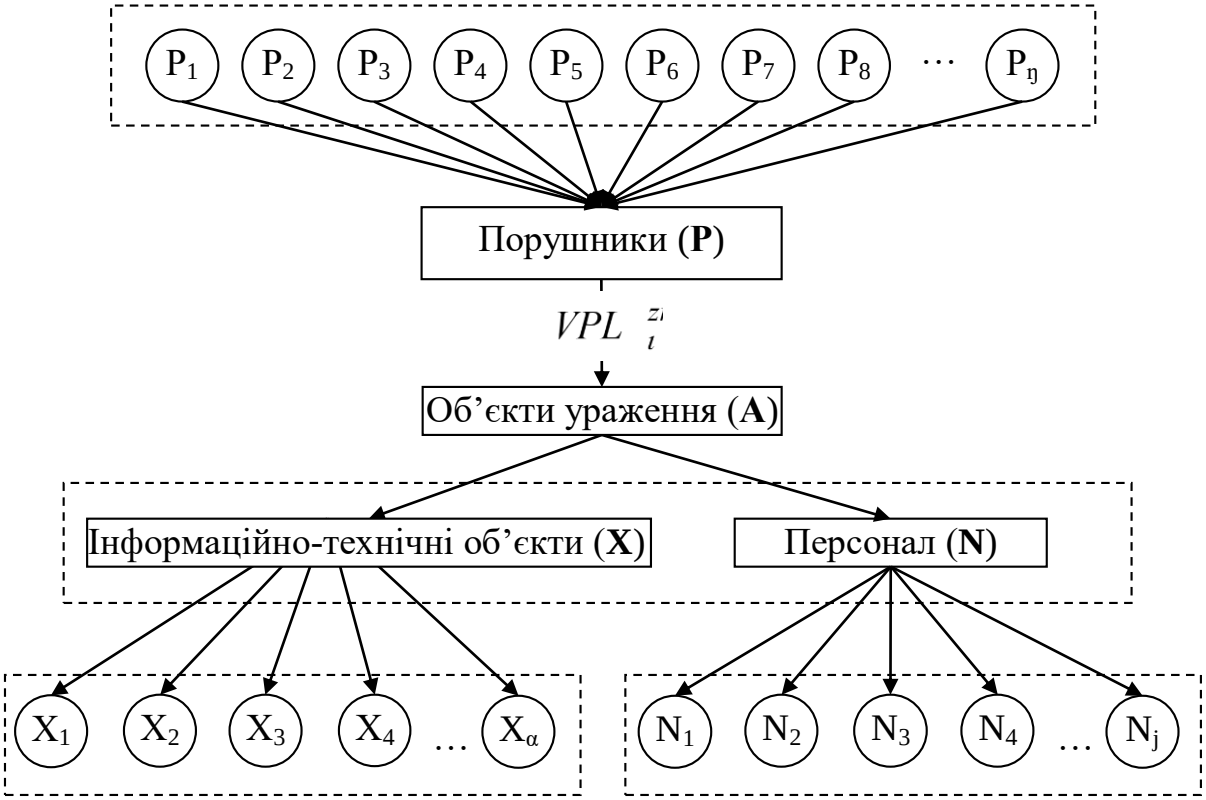


Рис. 2.3. Модель прояву порушників

Виходячи з рис. 2.3, маємо відкрите класифікаційне угрупування об’єктів ураження, представлене у вигляді об’єднання множин потенційних цілей порушника:

$$\mathbf{A} = \mathbf{N} \cup \mathbf{X} = (N \setminus X) \vee (X \setminus N) \vee (X \wedge N) \qquad (2.1)$$

Таким чином, визначено джерела небезпеки у вигляді множини порушників (**P**), які можуть здійснити напад (впливи) VPL^{zn} на об’єкт охорони з метою знищення або захоплення інформаційно-технічних об’єктів (**X**) або (та) персонал (**N**).

У результаті проведених досліджень сформовано множину небезпек НСД $\mathbf{S}$. НСД S_θ визначається на множині об’єктів ураження **A** наступним співвідношенням:

$$S_\theta = \{A_\sigma \mid \sigma = \overline{0,(X_a + N_j)}\} \tag{2.2}$$

НСД, що ви значена на об'єкті ураження S_θ визначається на множині порушників **P** наступним співвідношенням:

$$S_\theta^p = \{P_n \mid n = \overline{0, m_{sz}}\} \ , \tag{2.3}$$

де m_{sz} – кількість порушників.

НСД, що визначений на об'єкті ураження та множині порушників S_θ^p визначається на множині впливів, які ці порушники можуть здійснити:

$$S_\theta^{pv} = \{VPL_\iota^{zn} \mid \iota = \overline{0,k}\} \ , \tag{2.4}$$

де *k* – кількість ймовірних впливів.

Множина ймовірних подій визначається на множині ймовірних впливів на множині порушників і визначається із співвідношення:

$$T = (P \wedge VPL^{zn}) \tag{2.5}$$

НСД, що визначений на об'єкті ураження, множині порушників та множині ймовірних впливів визначається на множині засобів виявлення:

$$S_\theta^{pvs} = \{H_y, F_i, G_k \mid \theta = \overline{1,\mu}, y = \overline{1,\psi}, i = \overline{1,n}, k = \overline{1,\delta}\} \ , \tag{2.6}$$

де *n, δ, ψ* – кількість засобів виявлення кожного класу, μ– кількість рішень системи.

Таким чином, інформаційний вектор НСД можна представити у вигляді:

$$I_{\mu_i}^{pvs} = \{T_\upsilon, VPL_\iota^{zn}, P_n, A_\sigma \mid \upsilon = \overline{0,\xi}, \iota = \overline{0,c}, \sigma = \overline{0,(X_a + N_j)}, n = \overline{0, m_{sz}}\} . \tag{2.7}$$

Таким чином, S_θ^{pvs} визначається як інтегральний показник $W_i^{'}$, $i = \overline{0,\mu}$:

$$S_\theta^{pvs} = f(H_y, F_i, G_k) \tag{2.8}$$

Відповідно до (2.8) S_θ^{pvs}, визначається наявність НСД на територію та приймається рішення про генерування сигналу тривоги. Для ранжування порушника за принципом небезпечності, який здійснив НСД до периметру об'єкту

охорони введемо множину **R**, яка є підмножиною множини **Q** та має ті ж самі параметри.

2.3. Метод побудови блоку прийняття рішень із виявлення несанкціонованого доступу

Метод побудови блоку прийняття рішень з виявлення несанкціонованого доступу до периметру об'єкту охорони будуємо із використанням продукційної моделі представлення знань, що являє собою сукупність лінгвістичних висловів типу ЯКЩО <входи>, ТО <виходи>. Враховуємо, що ваги всіх експертних правил «ЯКЩО – ТО» дорівнюють одиниці.

Оскільки формалізовані знання експертів у початкових умовах можуть бути недостатніми, то передбачено, що матриця знань може піддаватися довчанню у міру появи нових знань про можливості виявлення НСД, експериментальних даних, шляхом уведення нових правил, які наблизять метод виявлення загроз НСД до реальних залежностей. Таким чином, передбачається адаптування або настроювання матриці знань.

Тому результат виявлення порушників НСД на території об'єкту охорони можна представити у вигляді:

$$S_{\theta}^{pvs} = f_{\theta}(H_y, G_k, F_i),\ \theta = \overline{1,\mu},\ y = \overline{0,\psi},\ k = \overline{0,\delta},\ i = \overline{0,n} \qquad (2.9)$$

де H_y – набір дискретних сигналів від датчиків руху, F_i – сигнал RFID-мітки *i*-го співробітника, G_k – потік даних, що надходить від камер, $f_{\theta}(H_y, G_k, F_i)$ – логічні висловлювання, що визначають категорію небезпеки НСД за принципом небезпечності $S_{\theta}^{pvs}, \theta = \overline{1,\mu}$.

Області зміни характеристик стану датчиків руху $H_y \in \left[\underline{H_y}, \overline{H_y}\right],\ y = \overline{1,\psi}$, RFID-міток $F_i \in \left[\underline{F_i}, \overline{F_i}\right],\ i = \overline{1,n}$, потоку відеоданих $G_k \in \left[\underline{G_k}, \overline{G_k}\right],\ k = \overline{1,\delta}$ та вихідного значення результату класифікації (ідентифікації) ситуації

$S_\theta^{pvs} \in \left[\underline{S}, \overline{S}\right]$, $\theta = \overline{1,\mu}$ відомі. Тут $\left[\underline{H_y}, \overline{H_y}\right]$, $\left[\underline{F_i}, \overline{F_i}\right]$, $\left[\underline{G_k}, \overline{G_k}\right]$ відповідно нижнє та верхнє значення характеристики стану датчиків руху, наявність/відсутність RFID-міток та наявність/відсутність даних відеокамер, що набувають значення 0 або 1.

Тоді, для фіксованого стану H_y, F_i, G_k визначеного фіксованим вектором вхідних параметрів у відповідність ставиться рішення S_θ^{pvs*}. Враховуючи вищезазначені чинники, отримуємо матрицю знань, що використовується для класифікації загрози появи несанкціонованого доступу та представлена в табл. 2.1.

Таблиця 2.1

Матриця знань, що використовується для класифікації загрози появи несанкціонованого доступу

№ вхідної комбінації значень	Вхідні змінні			Вихідна змінна
	Сигнали від датчиків руху (H_y)	Сигнал від RFID-міток (F_i)	Потік відеоданих (G_k)	S_θ^{pvs}
1	0	0	0	S_1
2	0	1	1	
3	1	1	1	
4	1	1	0	S_2
5	1	0	0	
6	1	0	1	
7	0	0	1	
8	0	1	0	

1. Розмірність цієї таблиці рівна (λ+1)×N, де (λ+1) – число стовпців, яке дорівнює кількості класифікаційних груп показників захищеності периметру позиції, N – кількість рядків.

2. Перші λ стовпців матриці відповідають вхідним змінним H_y, F_i та G_k, а (λ+1)-ий стовпець відповідає значенням S_θ^{pvs} вихідної змінної **S**, $\theta = \overline{1,\mu}$

3. Кожний рядок матриці являє собою деяку комбінацію значень вхідної змінної, що відноситься до одного з можливих значень вихідної змінної $\mathbf{S}$. При чому перші k_{θ_1} рядків відповідають значенню вихідної змінної S_1, другі $k_{\theta_2} - S_2$.

4. Вхідні змінні є бінарними. Елемент матриці $\alpha_\mu{}^e$, що стоїть на перетині рядка зі стовпцем, відповідає лінгвістичній оцінці параметру вхідних змінних та бере участь у визначенні можливого значення вихідної змінної $\mathbf{S}$, яка виявляє НСД.

Категоризація виявлення наявності НСД $\mathbf{S} = \bigcup_{\theta} S_\theta^{pvs}$, $\theta = \overline{1,2}$ містить наступні класифікаційні одиниці: $S_1 = S_1^{pvs}$ – сигнал тривоги не генерується; $S_2 = S_2^{pvs}$ – сигнал тривоги генерується.

Уведена матриця знань визначає систему логічних висловів типу «ЯКЩО – ТО, ІНАКШЕ», що зв’язують значення вхідних змінних з одним із можливих рішень, у даному випадку, визначає наявність визначає наявність несанкціонованого доступу до району чергового підрозділу, за формулою:

$$\text{IF [(H=1) AND (F=1) AND (G=1)] OR [(H=0) AND (F=0) AND (G=0)] OR [(H=0) AND (F=1) AND (G=1)] THEN S=S1, ELSE, S=S2} \quad (2.10)$$

Таким чином, запропоновано метод побудови блоку прийняття рішень з виявлення несанкціонованого доступу до периметру об’єкту охорони шляхом проектування та налаштування бази знань, що становить собою сукупність лінгвістичних висловів типу ЯКЩО <входи>, ТО <виходи>.

Якщо розташування чергового підрозділу є постійним місцем, і існує можливість розширити захищений периметр шляхом розподілу детекторів руху, RFID-міток та камер, наскільки це можливо з'являється можливість реалізації класифікації порушників.

2.4. Реалізація IoT системи охорони периметру засобами комп'ютерного моделювання

Для реалізації запропонованих моделей побудови IoT системи охорони периметру скористаємося програмним середовищем Cisco Packet Tracer [19-21]. Це багатофункціональна програма моделювання мереж, яка дозволяє експериментувати з поведінкою мережі і оцінювати можливі сценарії.

Припускаємо, що необхідно здійснити тимчасову охорону периметру при перевезенні вантажу/особи/ проведення розвідувальної операції. Створена засобами Cisco Packet Tracer імітація однієї зони охорони IoT система охорони периметру представлена на рис. 2.4. Дана схема містить комплект пристроїв, що використовуються для створення системи тимчасової охорони периметру.

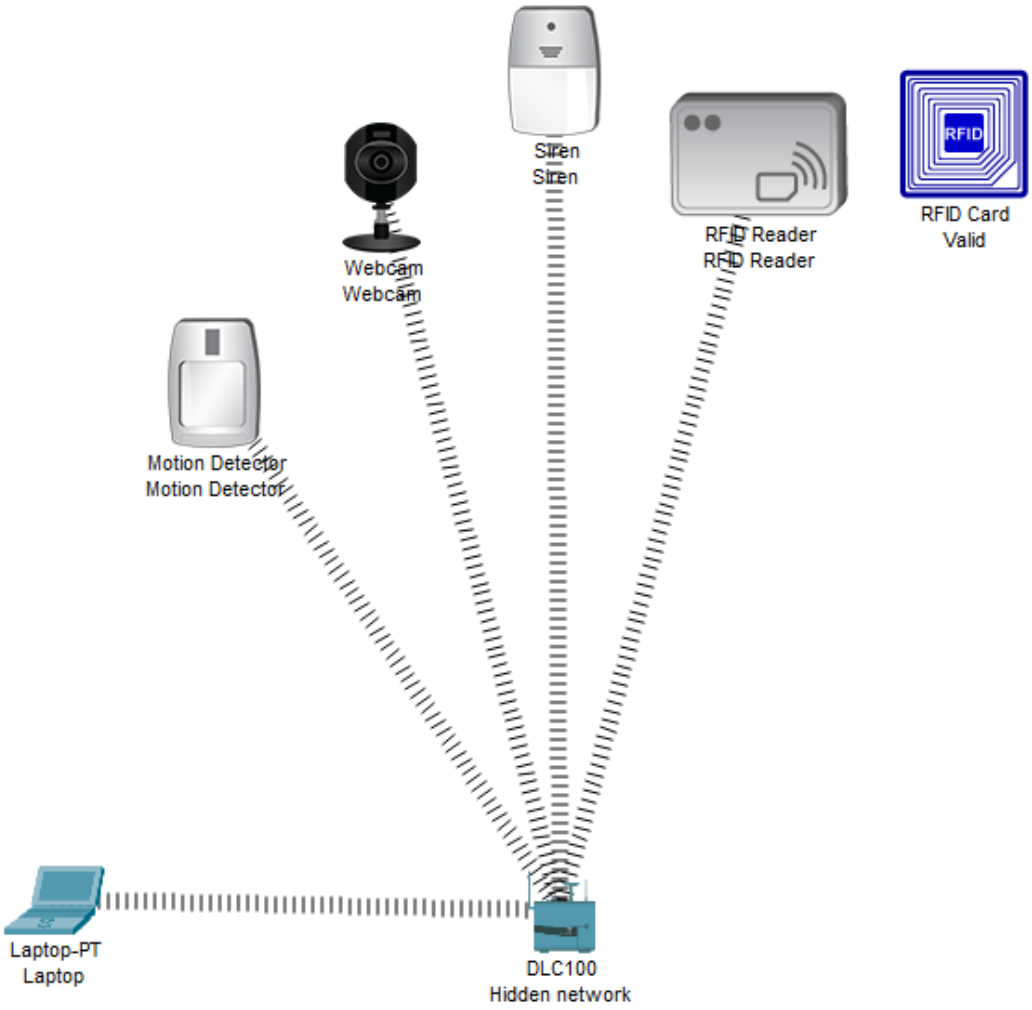


Рис.2.4. Кластер зони охорони

Да даного кластеру входить: відеокамера, датчик руху, сирена, RFID- зчитувач та RFID-картка, шлюз для прийому/передачі інформації та відповідно монітор IoT. Ці пристрої і є стандартними компонентами IoT системи охорони периметру.

Охорона об’єкту здійснюється в «польових» умовах, що вимагає ретельного підбору складових системи, підвищення вимог до їх працездатності та точності. Слід зауважити і на тому, що система повинна працювати з урахуванням рельєфу місцевості розгортання, бути непомітною для зловмисників, зручною у використанні, стійкою до параметрів навколишнього середовища та кібератак.

В залежності від території об’єкту охорони визначається необхідна кількість кластерів. Також на визначення кількості елементів системи впливають технічні характеристики вибраних засобів.

Проведено підключення всіх IoT пристроїв та налаштування роботи системи. На рисунку 2.5 представлено конфігураційні параметри налаштування RFID зчитувача та RFID мітки

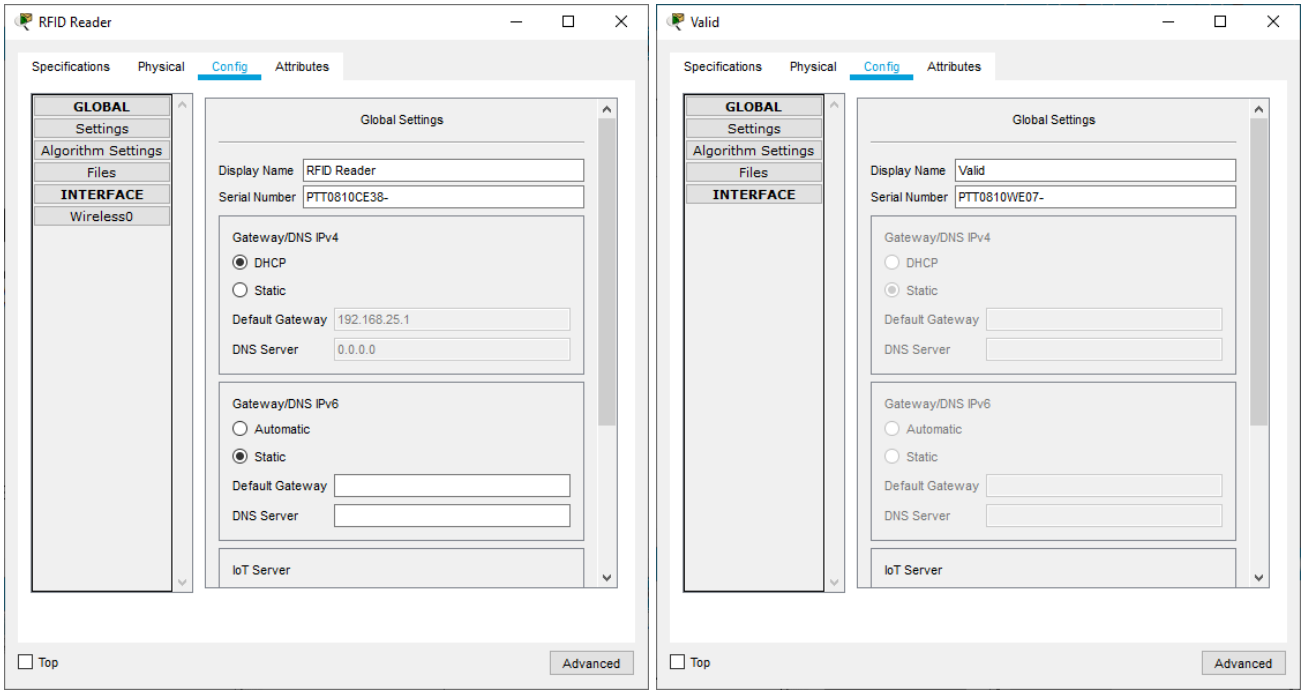


Рис. 2.5. Налаштування RFID зчитувача та RFID мітки

Проводимо налаштування відеокамери та сирени, рис. 2.6

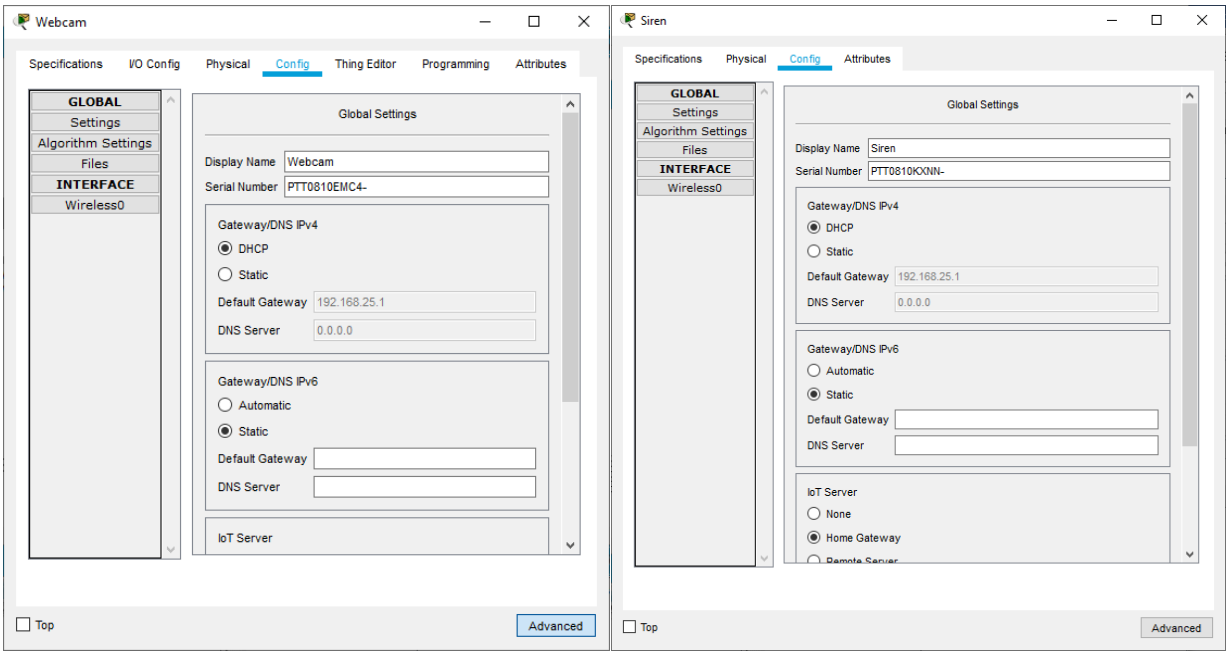


Рис.2.6. Налаштування відеокамери та сирени

Налаштування роботи датчику руху представлено на рис. 2.8

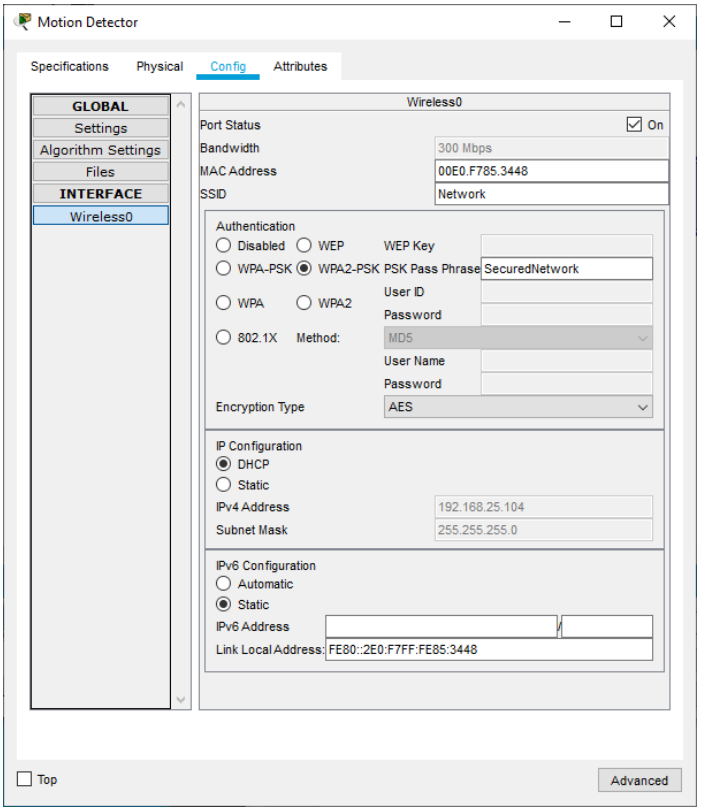


Рис. 2.8. Налаштування роботи датчику руху

Перелік підключених пристроїв до IoT монітору представлено на рис. 2.9. На рис.2.10 представлено налаштування шлюзу.

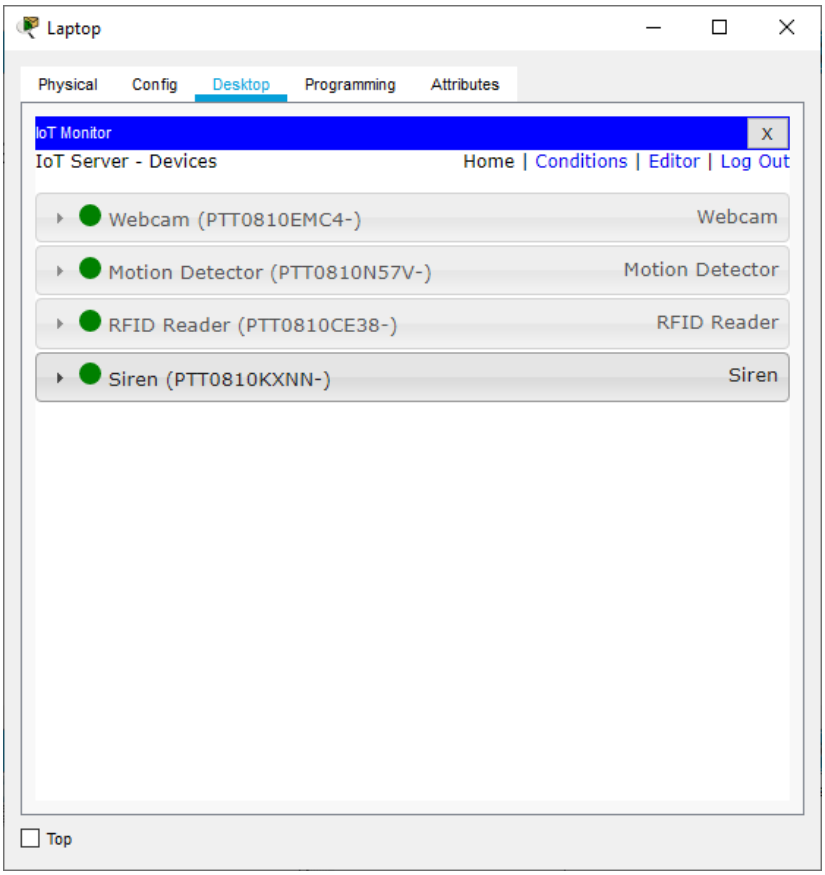


Рис.2.9. Перелік підключених пристроїв до IoT монітору

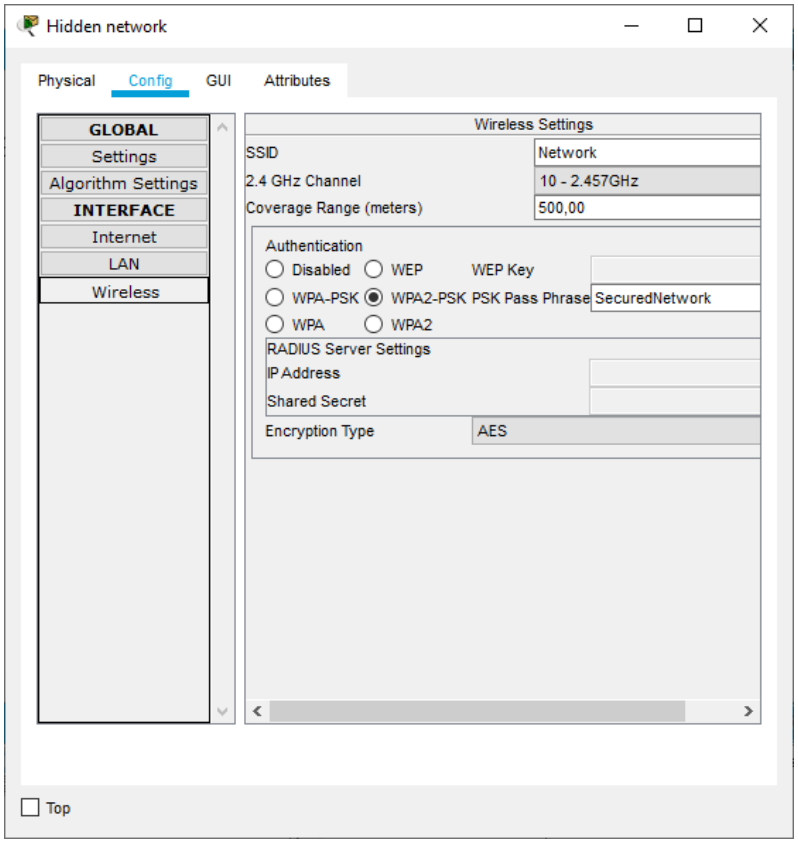


Рис.2.10. Налаштування шлюзу

Для коректної роботи IoT пристроїв, котрі підключені до IoT монітору є необхідність прописати умови увімкнення або вимкнення та режиму роботи того чи іншого датчика. Для цього у вкладці Conditions прописані правила, за якими функціонують IoT пристрої (Рис. 2.11).

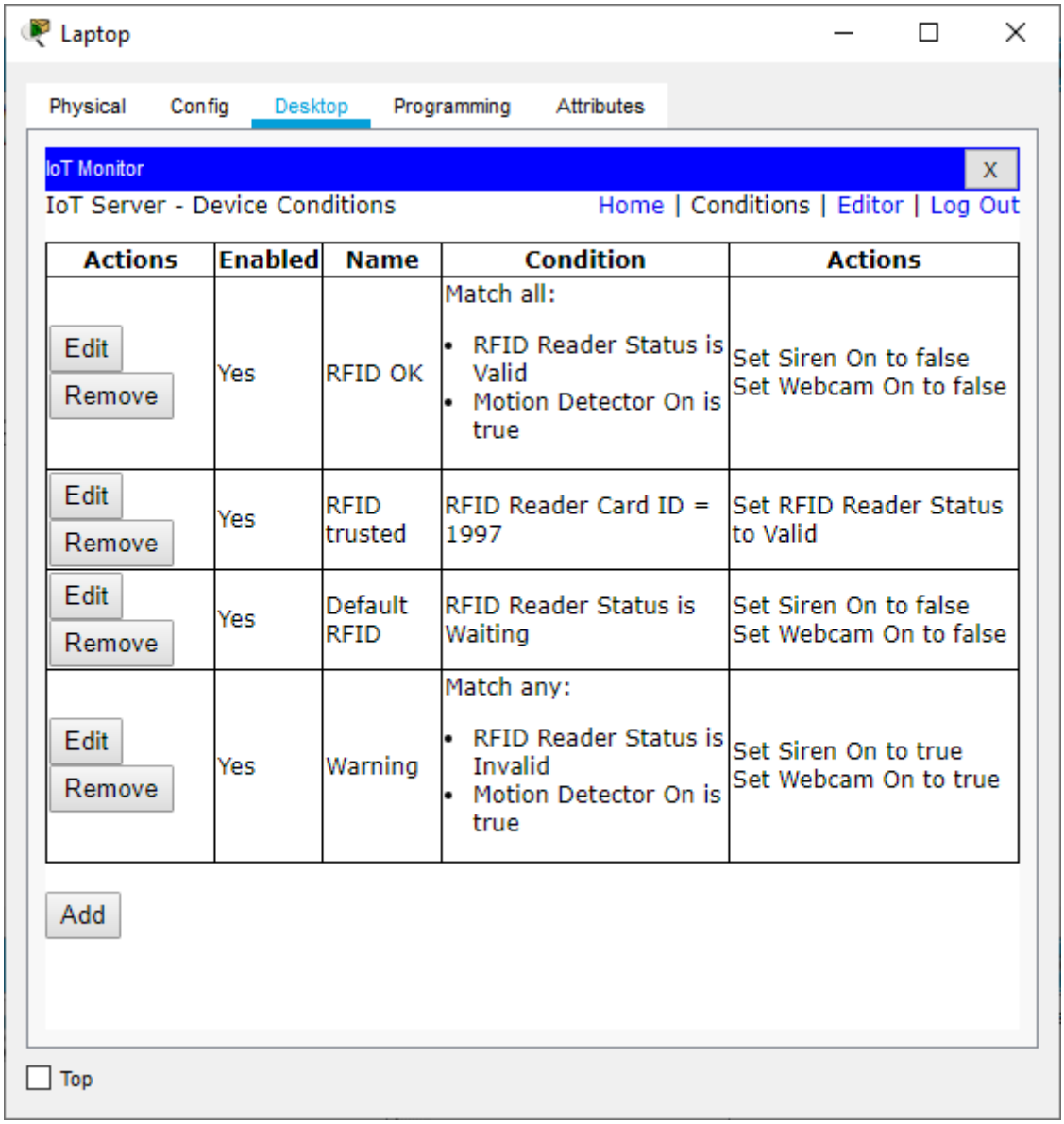


Рис. 2.11. Налагоджені правила роботи IoT системи

На наступному етапі проведемо діагностування працездатності системи. Перевіримо розпізнавання мітки та спрацювання датчику руху. При спрацюванні датчику руху повинна спрацювати сирена та включитись відеокамера, рис. 2.12-2.13.

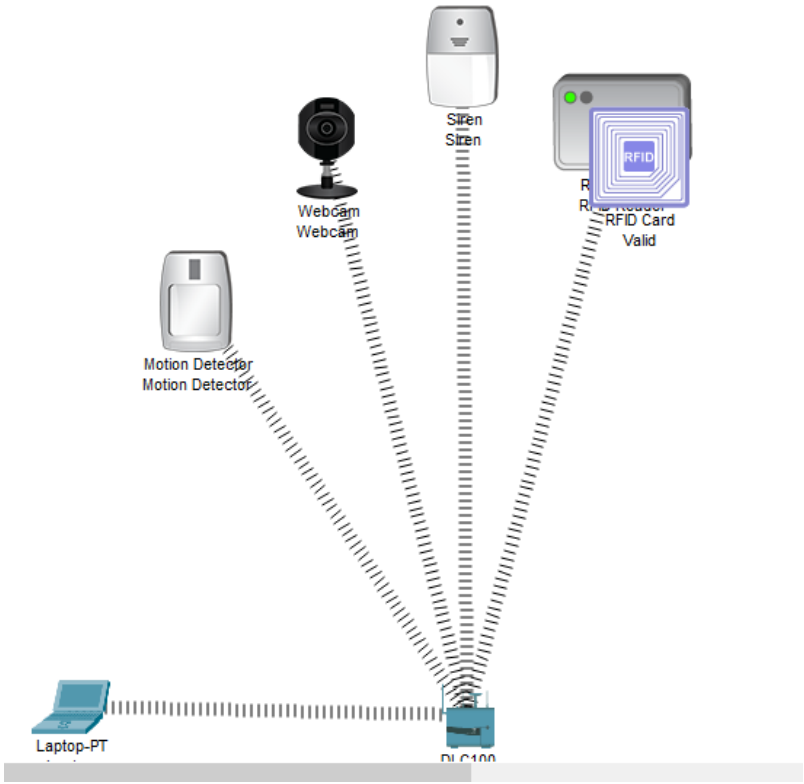


Рис.2.12. Розпізнавання RFID-мітки

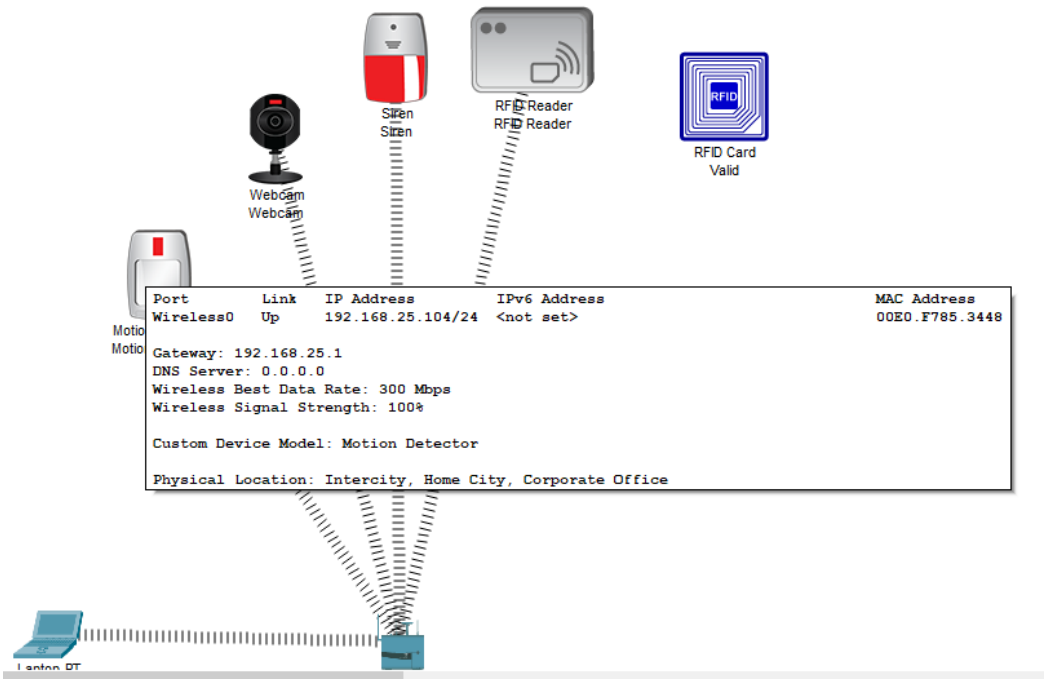


Рис.2.13 Спрацювання датчику руху

В залежності від задач, що будуть поставлені перед системою, система може мати різні конфігурації, наприклад, рис. 2.14-2.16.

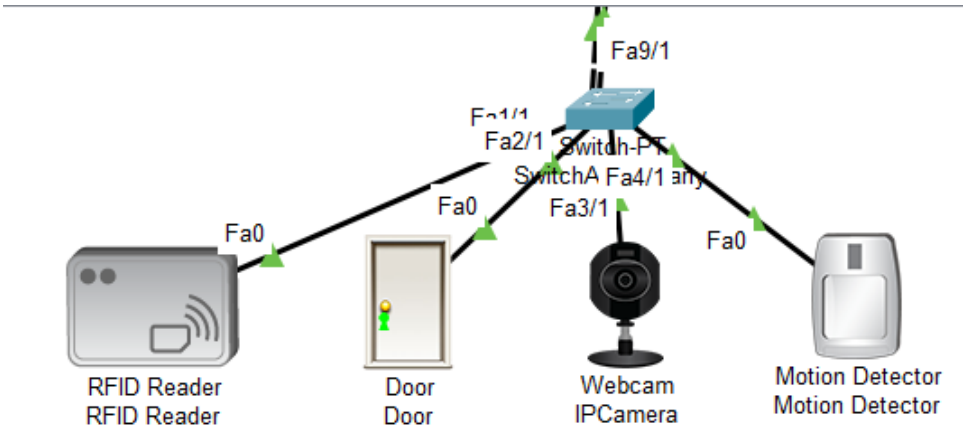


Рис. 2.14. Схема для контролю входу/виходу, а також здійснення моніторингу прилеглої території

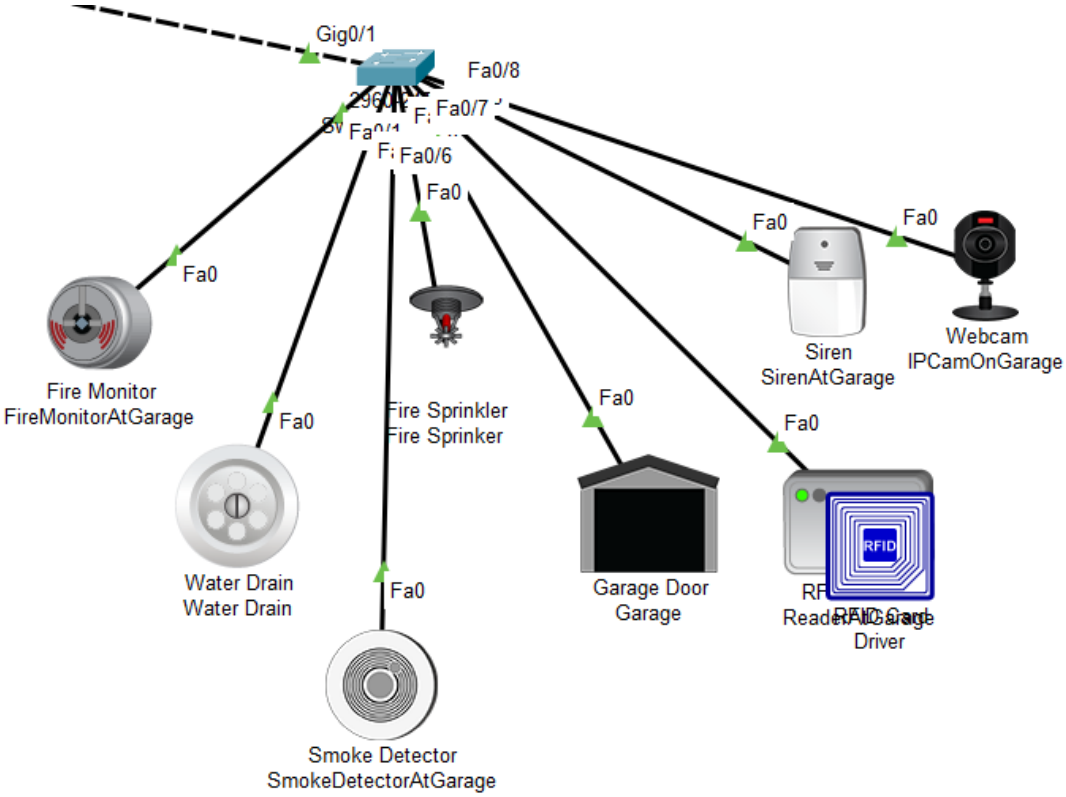


Рис. 2.15. Схема пожежно-охоронної сигналізації окремого приміщення на прикладі гаражу

Побудова комп’ютерна модель, рис.2.4 дозволяє нам визначити потенційні кіберзагрози та розробити технологію забезпечення кібербезпеки компонентів IoT.

Висновки до другого розділу

1. Запропоновано структуру IoT системи охорони периметру, яка включає в себе підсистему безконтактної радіочастотної ідентифікації (RFID) (Модуль 1); підсистему інтелектуального відеоспостереження (Модуль 2); СППР із виявлення та попередження НСД на території об’єкту охорони (Модуль 3); підсистему виявлення руху по контуру периметру захисту (Модуль 4). Інтеграція та реалізація цих підсистем дозволяють автоматизувати процес виявлення порушників та процес прийняття рішень щодо формування сигналу тривоги.

2. Запропоновано модель взаємодії компонентів IoT системи охорони периметру. Дана модель визначає інформаційні потоки та реалізує взаємодію компонентів системи. Також було визначено форму інформаційних векторів.

3. Запропоновано метод побудови блоку прийняття рішень з виявлення несанкціонованого доступу до периметру об’єкту охорони шляхом проектування та налаштування бази знань, що становить собою сукупність лінгвістичних висловів типу ЯКЩО <входи>, ТО <виходи>. Наведені вирази мають форму операцій нечіткої логіки та матриці знань, отже, є можливість автоматизувати процес визначення загроз.

4. Проведено комп’ютерне моделювання IoT системи охорони периметру засобами Cisco Packet Tracer дозволило перевірити працездатність запропонованих моделей та дозволяє нам визначити потенційні кіберзагрози для даної структури.

3. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ КІБЕРЗАХИСТУ КОМПОНЕНТІВ IoT СИСТЕМИ

3.1. Аналіз кіберзагроз компонентів IoT системи

Системи охорони периметру території є складними інтегрованими комплексами. Поєднання різних технологій та засобів різних виробників збільшує ймовірність виникнення кіберзагроз та зростання вразливостей системи. В межах даного дослідження проведемо аналіз кіберзагроз IoT системи короткотривалої охорони периметру режимного об'єкту, що розгортається в «польових» умовах та функціонує на бездротових мережах передачі даних. В структуру входить множина датчиків руху **H**, систем відеокамер **G** , RFID-зчитувачів та RFID-міток **F**, шлюз та безпесередньо IoT монітор у вигляді СППР системи.

Входження людства в четверту промислову революцію (INDUSTRY 4.0) [22] створює нові виклики та можливості для України. Нові кіберзагрози пов'язані з масовим використанням технологій INDUSTRY 4.0, що можуть спричинити катастрофічні наслідки при реалізації атаки на режимні об'єкти. Особливо актуально дана задача ставиться при організації тимчасової охорони периметру режимного об'єкту, коли є обмеження ресурсів, несприятливі погодні умови, непередбачений рельєф місцевості.

Найбільша кількість атак припадає на портативні пристрої, використання безпровідних технологій зв'язку між елементами системи створює передумови для здійснення кібератаки на систему. Відповідно до [22] НСД найчастіше здійснюється хакерами через точки входу (доступу) до корпоративної мережі або використовується для запуску DDoS-атаки. Враховуючи велику кількість датчиків, що підключаються до системи, використання бездротових мереж, хмарних сервісів і т.ін. не дозволяють забезпечити надійний периметр кіберзахисту об'єкту. Ще одним напрямком є викрадення конфіденційних даних користувачів (компаній). Потужний потенціал кіберзагроз мають технології машинного навчання та використання систем штучного інтелекту через подвійне призначення (алгоритми, що використовуються можуть як протидіяти кібератакам так і їх створювати). Нові

технології створюють нові кіберзагрози, протистояти яким можна лише з використанням нових інформаційних технологій.

Глобальна статистика, зібрана компанією Cisco у 2017 р. [22], свідчить про таке:

- уразливості («дірки») в сучасних системах захисту уможливлюють до 65 % кіберінцидентів;
- людський фактор – критичне (якщо масштабувати його до кількості та ступеня складності кіберзагроз) зниження рівня грамотності користувачів – до 48% інцидентів;
- 55 % організацій нездатні встановити причину інциденту;
- середній час встановлення такої причини в сучасній індустрії ІБ та кібербезпеки складає 100 днів.

Провідні компанії та спеціалісти впроваджують багатоступеневі комплексні системи захисту, що базуються на використанні новітніх технічних засобів, кваліфікованих кадрів, контрольних процедурах, адміністративних регламентах з чітким їх дотриманням. В такого роду системах акцент робиться на налагодженні систем раннього оповіщення, які забезпечують контроль функціонування IT-обладнання в режимі реального часу, повідомляють адміністраторів у разі виникнення будь-якої аномальної активності, дозволяють своєчасно виявляти атаки, а також аналізувати потенційні загрози . Критеріями стійкості такої системи захисту є здатність своєчасно і адекватно реагувати на атаки і відновлювати роботу об’єкту з мінімальними втратами [22].

Досліджувальна нами система є бездротовою IoT системою, апаратна частина якої може бути розділена на наступні елементи, рис. 1.3 [23-30]:

1) комунікаційна підсистема (бездротовий зв’язок в сенсорній мережі, включає в себе радіоприймач);
2) обчислювальна підсистема (обробка даних, функціональність вузла);
3) сенсорна підсистема (з’єднання мережі із «зовнішнім світом»);
4) підсистема електроживлення.

Рис. 3.1. Апаратна частина вузла IoT системи

Враховуючі ті задачі, які ставляться перед системою ставляться більш жорсткі вимоги до апаратного забезпечення:

- мале споживання електроенергії;
- можливість працювати з великою кількістю вузлів на відносно малих відстанях;
- відносно невелика собівартість;
- працювати автономно та без обслуговування;
- мати маскувальний ефект;
- бути стійкими до навколишнього природнього середовища.

Враховуючи той факт, що сенсорні мережі вразливі до безлічі атак, особливо актуально питання забезпечення кіберзахисту ставиться при впровадження IoT систем охорони периметру режимного об’єкту. Основою кібербезпеки IoT є:

- безпека зв’язку;
- захист пристроїв;
- контроль пристроїв;
- контроль взаємодії в мережі.

Проведемо аналіз атак, що можуть бути здійсненні відносно системи та базуючись на власному досвіді та проведених дослідженнях у [29-31], рис. 3.2:

✓ відмова в обслуговуванні (Denial-of-Service (DoS)):

фізичного рівня:

- атака постановки перешкоди;
- атака втручання в IoT системи;

канального рівня:

- атака зіткнень;

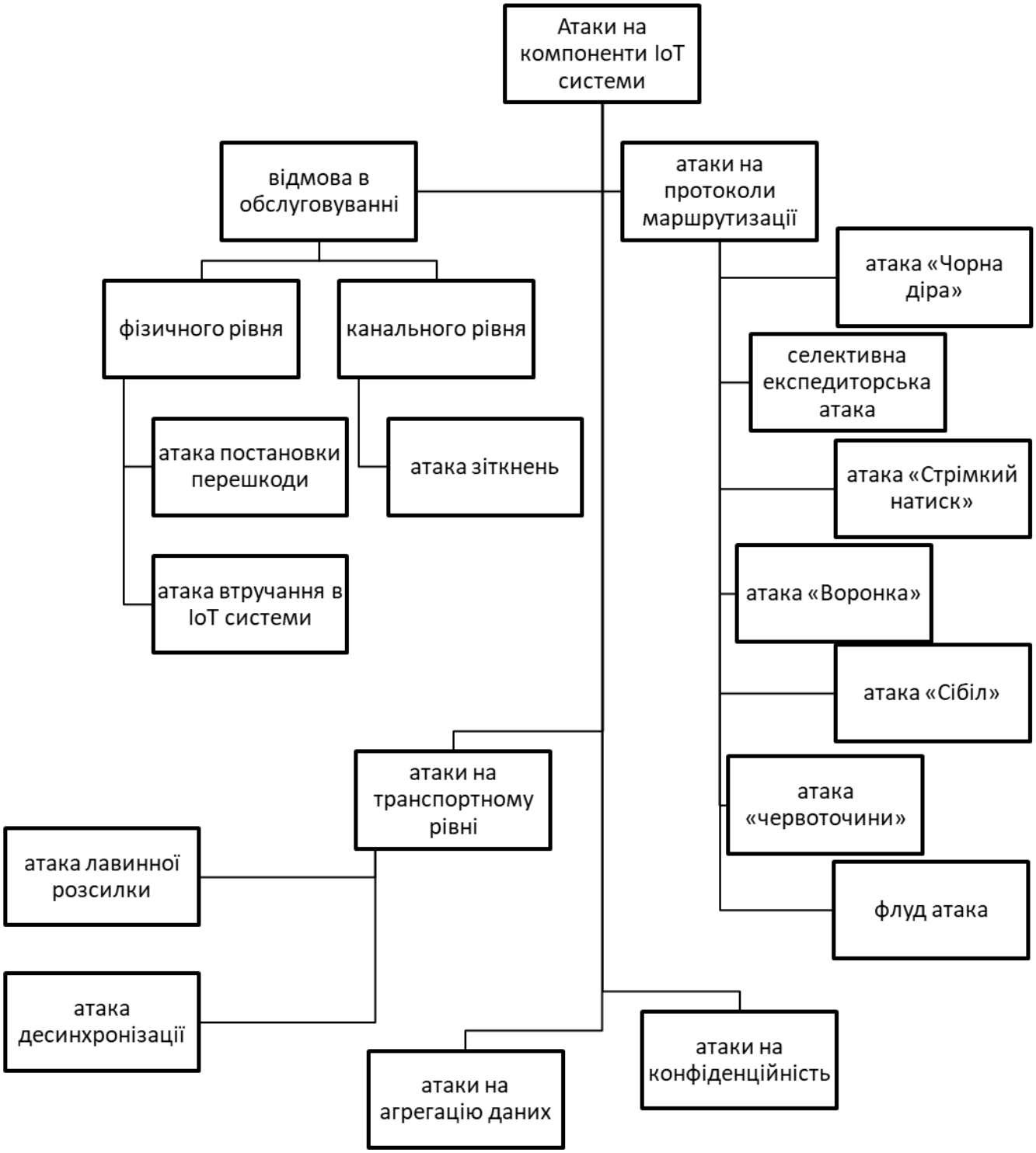


Рис. 3.2. Атаки на компоненти IoT системи

- ✓ атаки на протоколи маршрутизації:
  - атака «Чорна діра»;
  - селективна експедиторська атака;
  - атака «Стрімкий натиск»;
  - атака «Воронка»;
  - атака «Сібіл»;
  - атака «червоточини»;
  - флуд атака;
- ✓ атаки на транспортному рівні:
  - атака лавинної розсилки;
  - атака десинхронізації;
- ✓ атаки на агрегацію даних;
- ✓ атаки на конфіденційність.

DoS-атака на фізичному рівні. DoS-атака характеризується спробою противника зупинити функціонування мережі або руйнування служби безпеки мережі. У IoT системі DoS-атака може відбутися на різних рівнях стека протоколу, може впливати на декілька рівнів одночасно та використовувати взаємодію між ними. DoS-атака на фізичному рівні може здійснюватися при втручанні в радіочастоти на яких працює система. При такій атаці один атакуючий вузол може відключити всю мережу або якусь її частину (наприклад, блокування передачі даних).

Атака втручання в роботу IoT системи при виявленні сенсору (в нашому випадку датчика/камери по периметру об’єкту охорони) та намагання отримати фізично до нього доступ має критичне значення для нашої системи. В такому випадку зловмисник може знищити пристрій, спробувати підмінити дані, отримати доступ до конфіденційної інформації (зокрема криптографічні ключі), використовувати пристрій для входу в мережу.

DoS-атака канального рівня. DoS атака зіткнень на канальному рівні направлена, як правило на вичерпання ресурсів вузлів. Дана атака впливає на процес передачі пакетів, викликаючи процедури експоненціальної затримки та

повторної передачі пакетів в деяких протоколах MAC. Так, при пошкодженні великої кількості бітів в пакеті, вузол буде намагатися використати коди з виправленням (корекцією) помилки, щоб відновити пошкоджені біти, тим самим витрачаючи енергетичні ресурси, що є обмеженими. Іншим прикладом такої атаки є «зіткнення» в кінці фрейму, що призводить до повторної ретрансляції всього пакету. Ще одним варіантом здійснення атак, що притаманний протоколам IEEE 802.11 може бути генерація RTS-повідомлення на базову станцію або сусідній вузол, що призведе до обробки даного повідомлення та генерування CTS повідомлення, далі йде очікування прийому сигналу, причому всі інші вузли припиняють передачу даних на приймаючих вузол на час, що зазначений у RTS-повідомленні. Також можуть реалізовуватися методи квітирування.

Проведемо аналіз **атак на протоколи маршрутизації**. Відома атака «Чорна діра» направлена на використання протоколу маршрутизації для перенаправлення пакетів, що йдуть від або до цільового вузла, через певний вузол. Ця атака може використовуватися для викидання пакетів або «людина посередині» (метод компрометації каналу зв’язку, при якому зловмисник, приєднавшись до каналу між контрагентами, здійснює втручання в протокол передачі, видаляючи або змінюючи інформацію). Іншим видом атаки є селективна експедиторська атака, яка схожа з атакою «Чорної діри», однак в даній атаці відкинутими будуть пакети, які задовольняють певним критеріям, а не всі.

При реалізації атаки «Стрімкий натиск» використовується процедура відкриття маршруту на вимогу протоколів маршрутизації. Шкідливий вузол генерує та передає запит маршруту своїм сусідам, і в результаті у вузла зростає ймовірність бути частиною обраного маршруту між джерелом та пунктом призначення.

Атака «Воронка» характерна тим, що зловмисник намагається, або скомпрометований вузол, або розмістити свій на шляху якомога більшої кількості потоків мережі і той, далі починає діяти по типу воронки – збираючи весь трафік сенсорної мережі. В протоколах, що використовують широкомовну розсилку, зловмисник прослуховуючи канал, повідомляє сусідів про те, що «знає»

найкоротший маршрут до базової станції. Як тільки йому вдалося стати між транслюючим сенсорним вузлом і базовою станцією, він може виконувати будь-які дії з пакетам даних, що надходять до нього.

Атака «Сібіл» характеризується тим, що зловмисник намагається скомпрометувати діючий вузол, або підключити свій маючи декілька псевдоіндентифікаторі і тим самим видаючи себе за декілька вузлів одночасно. Таким чином сусідні вузли можуть сприйняти його за «свого». Такого роду атаки використовуються для порушення механізму розподіленого зберігання, механізмів маршрутизації, механізмів агрегації даних, механізмів голосування в мережі.

Атака «червоточини» представляє серйозну загрозу безпеці сенсорних мереж через те, що вона не вимагає компрометації сенсорного вузла. Так, наприклад атакуючий прослуховує канал і отримує трансляцію розсилки для запиту маршруту від базової станції і перенаправляє його до найближчого сусіда. Вузол, що отримав дане повідомлення буде вважати його батьківським, тобто таким, що знаходиться найближче від нього, хоча це зовсім не так. Дія атаки базується на створенні спеціального шляху між двома і більше вузлами мережі для передачі перехоплених пакетів, причому вузли будуть думати, що передають пакети найкоротшим шляхом.

Є одним різновидом атаки є флуд атака (HELLO flood attack). Особливістю даної атаки є намагання передати у мережу масу необов’язкових повідомлень, які позбавлять мережу різноманітних ресурсів (обчислювальної потужності, канальної ємності, енергетичних ресурсів). Маючи високочастотний радіопередавач з достатньою обчислювальною потужністю зловмисник проводить розсилку Hello пакетів безлічі вузлів сенсорної мережі. Отримавши дане повідомлення вузли сприймають скомпрометований вузол як сусіда і включають отриману адресу відправника в розсилку. Таким чином зловмисник отримує доступ до даних, що відправляються з вузлів.

До функцій транспортного рівня відносять здійснення доставки пакетів (TCP) та дейтаграм (UDP) від відправника до одержувача. **Атаки на транспортному рівні** направлені на аналіз регулярності трафіку і посилка паралельних дублікатів

повідомлень по інших шляхах, що використовуються на даному рівні. Враховуючи той факт, що більшість транспортних протоколів підтримують конфіденційну інформацію і тому уразливі до виснаження пам’яті, атака лавинної розсилки (зловмисник робить нові запити на встановлення з’єднання кожного разу збільшуючи кількість конфіденційної інформації в атакуючих вузол, поступово призводячи до того, що вузол стає несправним (відмова вузла від подальших з’єднань) через вичерпання ресурсу) і використовує цей недолік.

Ще однієї характерною атакою цього рівня є атака десинхронізації, в результаті якої зловмисник намагається зруйнувати зв'язок між двома робочими вузлами в мережі, неодноразово підробляючи повідомлення до них. Зокрема протоколи транспортного рівня можуть використовувати порядкові номери для відстеження успішно отриманих пакетів, ідентифікації пакетної втрати та виявлення копій. Згенеровані зловмисником пакети, можуть використовувати ці порядкові номери, щоб запевнити вузол в тому, що пакети були втрачені та спровокувати повторну передачу, що може мати віомі нам вже наслідки вичерпання ресурсу та заповнення каналу передачі даних, коли дійсна інформація не надходить до бази, або надходить із запізненням.

Атаки на агрегацію даних направлена на зміну поведінки мережі. Процедури агрегації та злиття даних використовуються в мережах, де розміщення типових сенсорів є близьким один до одного. Такі процедури використовуються для об’єднання багаторазових даних з метою усунення надлишкової інформації. В цілях економії ресурсів це позитивно, однак є небезпечною зі сторони кібербезпеки. Так обрахунок простих математичних функцій (мінімум, максимум, середнє значення, сума), що використовуються при агрегації у разі присутності одного шкідливого вузла або заміні реальних даних з сенсорів може змінити поведінку мережі частково або в цілому.

Атаки на конфіденційність направлення на заволодіння інформацією, що зібрана сенсорами і можуть бути реалізовані за рахунок прослуховування мережі, аналіз трафіку або/та заволодіння вузлом. Особливо актуально це для тих мереж, же не використовується шифрування даних.

3.2. Рекомендації з протидії атакам на компоненти IoT системи

Протидія DoS атакам фізичного рівня. Використання стандартів IEEE 802.11 (широкосмуговий зв'язок) використовують стрибкоподібну перебудову частоти роботи. В такому випадку передавач перешкоди повинен «знати» послідовність стрибкоподібного руху або створити перешкоду більшої смуги частот. Пропонується використовувати технологію розширення спектру для захисту від подібних атак. Передача такого сигналу буде схожа на шум, що дозволить знизити ризики навмисного інтерференційного впливу на інформаційний сигнал.

Крім того при зникненні сигналу від будь-якої ділянки мережі або вузлу, елементу мережі, СППР повинна генеруватися тривогу по підрозділу. Вузли, які виявили атаку перешкоди, повинні передати коротке повідомлення своїм «сусідам» та на базову станцію про атаку на мережу. В такому випадку, якщо повідомлення «не дійде» до базової станції від атакованого вузла, то існує ймовірність отримання аварійного повідомлення від вузла, що не зазнав атаки.

Для протидії атакам втручання в роботу IoT системи кожен датчик, що використовується в системі необхідно оснастити тампером (мініатюрна кнопка на платі пристрою, що віджимається при відкриванні корпусу або його від'єднанні від місця кріплення). При спрацюванні тампера, хаб відправляє всім користувачам системи безпеки push-повідомлення та SMS (при наявності такого типу повідомлень у пристроях, що будуть використовуватись), а також передачу повідомлення на базову станцію. Крім того, бажано передбачити програмно, що при спрацьовуванні тампера при «постановці на охорону», всі дані, що зберігаються на пристрої знищувалися автоматично. Для уникнення виявлення датчиків, їх слід розміщувати у скритних місцях, але придатних до їх встановлення, використовувати матеріали, стійкі до зовнішніх впливів. Датчики та камери мають свій радіус дії, тому при розміщенні таких пристроїв слід враховувати цей показник та встановлювати їх з перекриттям для уникнення зони нечутливості. При правильному встановленні, датчик виявить небезпеку та відправить сигнал тривоги на базову станцію до того моменту, як зловмисник до нього наблизиться впритул.

В запропонованій системі використовується RFID-мітка для ідентифікації особи. В СППР передбачена ситуація, коли спрацьовує RFID-мітка та датчик руху, однак ми не отримуємо сигнал від відеокамери. Ця ситуація може говорити про наступне, що мітка була «вилучена» або «підмінена» і датчик руху виявив рух, однак зловмисники могли вивести з ладу камеру, щоб уникнути виявлення себе як порушників. Даний набір параметрів згенерує сигнал тривоги по підрозділу.

Для протидії DoS-атака канального рівня є аутентифікація для перевірки того, що вузол, що генерує повідомлення авторизований у мережі у поєднанні з шифруванням. В нашому випадку ми використовуємо стандарт аутентифікації WPA2-PSK з типом шифрування AES. Враховуючи ліміт енергоресурсів використання асиметричного шифрування стає неможливим в такого роду системах. Головний недолік використання симетричного шифрування – це проблема розподілу ключів. При використанні симетричної криптографічної схеми необхідно забезпечити надійне і безпечне встановлення спільно використовуваних криптографічних ключів між двома вузлами, перш ніж вони зможуть обмінюватися даними. Техніка встановлення та управління ключами повинні бути придатними для використання з сотнями і тисячами вузлів.

Ще одним напрямком удосконалення захисту є встановлення RFID-мітки на всіх пристроях мережі та проведення комбінованої (двофакторної) процедури аутентифікації вузлів.

Пропонується використання технологію блокчейн для захисту від втручання в код програми та підміну показників датчиків. Дана технологія є розподіленою базою даних, яка потенційно доступна кожному. Завдяки використанню технології блокчейн можна протидіяти шахрайству, проводити управління ідентифікацією, транзакції, верифікацію стану елементів різних систем, забезпечити цілісність даних. Комбінування технологій блокчейн та Інтернет речей можна вирішити ряд проблем з безпекою, а саме: відстеження вимірювань даних сенсора та запобігання дублюванню будь-якими іншими шкідливими даними; автентифікація та безпечна передача даних.

Для забезпечення потреб захисту від прослуховування, ін’єкцій і модифікації

пакетів пропонується використання криптографії.

Для протидії атакам агрегації пропонується використання методи затримки агрегації та аутентифікації. Для запобігання атакам маршрутизації використовуємо шифрування на канальному рівні і аутентифікацію з використанням глобального загального ключа. Атакам «Сибіл» можна запобігти шляхом перевірки ідентичності сенсорних вузлів (використання спільного симетричного ключа з довіреної базової станції) та обмеженні числа сусідів, які може мати вузол. Таким чином скомпрометований вузол зможе зв'язатися тільки з перевіреними сусідами. Протидіяти атаці «Воронка» можна використовуючи протокол географічної маршрутизації, при якому трафік «природньо» спрямований до фізичного розташування базової станції важко піддається перенаправленню для створення воронки.

Запропонована система використовує статичні датчики, які потребують одноразової автентифікації в мережі.

3.3. Модель підсистеми моніторингу інцидентів кібербезпеки в IoT системах

Як відомо, в роботі сучасних систем моніторингу інцидентів виділяються наступні етапи: визначення інциденту; сповіщення про виникнення інциденту; реєстрація інциденту; усунення наслідків і причин інциденту; розслідування інциденту; реалізація дій, що застерігають повторне виникнення інциденту. За даними аналізу сучасних систем, для забезпечення управління інцидентами система повинна виконувати наступні функції:

1. Контроль зовнішніх пристроїв, що підключаються, зокрема можливість в режимі online контролювати підключення нових вузлів.

2. Моніторинг вузлів і їх захист, зокрема можливість в режимі online контролювати вузли, можливість налаштування реагування на події, захист вузлів від видалення або виключення, контроль цілісності.

3. Управління системою та обробка інцидентів, зокрема наявність власної

консолі, розподіл ролей адміністратора і спеціалістів з безпеки, налаштування сповіщень, можливості реагування на інциденти, аналіз подій, зафіксованих системою, збереження історії інцидентів для наступного аналізу, заборона на пропуск затриманого повідомлення або дозвіл із записом про інцидент.

4. Формування системи звітності про роботу системи управління інцидентами, зокрема можливість побудови звітів про порушення, наявність варіантів отримання звітів про порушення, тимчасовий запис звіту в локальне сховище у разі недоступності сервера, експорт звітів, запис в журнал реєстрації дій адміністраторів системи.

Основним завданням даного дослідження є розробка системної моделі моніторингу інцидентів. Згідно з переліком функції системи управління інцидентами її можна віднести до систем моніторингового типу.

Отже для розробки математичної моделі її функціонування можна використати методи ідентифікації систем відповідного класу. В дослідженні обмежимося формалізацією процесу моніторингу інформаційної системи та визначення типу інциденту.

Розглянемо узагальнену схему системи моніторингових спостережень, що включає (рис. 3.3):

1. Кінцеву групу об’єктів моніторингових спостережень системи $V_1,\ldots V_N$ в абстрактному обмеженому просторі W. Такими об’єктами системи моніторингу інцидентів є:

• апаратні засоби (сенсорні вузли, базові станції, шлюзи);

• програмні комплекси (операційні системи, антивірусні шлюзи, підсистеми обробки даних, доступні служби та сервіси);

• інформаційні ресурси (бази даних, файли, що доступні в мережі, тощо);

2. Кінцеву групу зовнішніх об’єктів спостережень системи $U_1,..,U_M$ в обмеженому просторі Ω . Такими об’єктами є: мережні потоки даних, зовнішні повідомлення тощо.

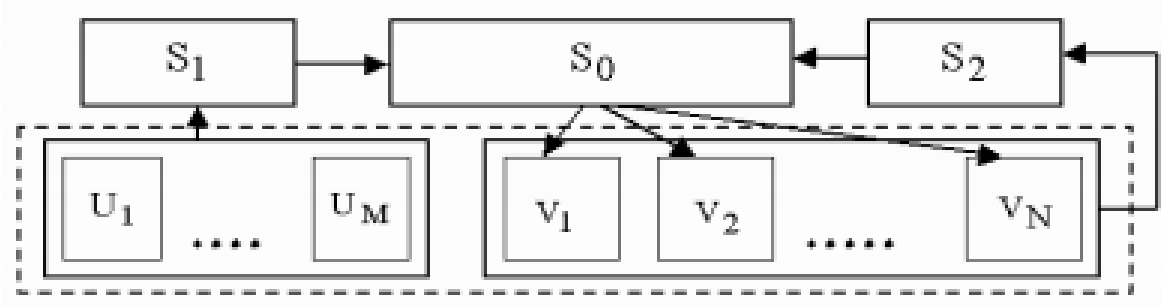


Рис. 3.3. Формальна схема системи управління інцидентами кібербезпеки

3. Підсистему S_1 спостережень над об'єктами U_1 ,.., U_M , збору і представлення зовнішніх (некерованих) параметрів системи. До некерованих параметрів системи відносяться запити на доступ від вузлів, що не пройшли встановлену процедуру автентифікації, кількість запитів в одиницю часу, заявки на обслуговування певних типів, несанкціонований доступ до інформаційних ресурсів, деструктивні дії резидентних програм та зловмисників тощо.

4. Підсистему S_2 спостережень над об'єктами O_1 ,.., O_N, збору і представлення внутрішніх (керованих) параметрів системи. До керованих параметрів відносяться інформація про роботу вузлів та інформація щодо доступності служб і додатків (за наявності).

5. Підсистему S_0 аналізу і прогнозування стану системи, в якій ухвалюється рішення про управляючі дії на об'єкти моніторингу.

Для подальшого аналізу введемо наступні позначення:

а) для програмних комплексів (O_1): доступність служби – O_{11} ; наявність помилки в роботі додатків – O_{12} ; дисковий простір вичерпано – O_{13} ;

б) для устаткування (O_2): збій системи – O_{21} ; внутрішній сигнал тривоги – O_{22} ; відмова вузла – O_{23} ;

в) для зовнішніх повідомлень (O_3): надходження заявки на отримання додаткової інформації – O_{31} ; запит на забутий пароль – O_{32} ;

г) для інформаційних ресурсів (O_4): спроба несанкціонованого доступу – O_{41}; знищення інформації – O_{42} ; зміна інформації – O_{43}.

Результатами роботи даної підсистеми є визначення ймовірності інциденту,

його документування та вибір дій щодо усунення. Для визначення її ефективності необхідною є оцінка функціонування системи за визначеними нижче параметрами: своєчасна реєстрація (аудит) подій різних типів (U_1), що оцінюється за множиною типів подій (показники (U_{1i})); визначення рівня достовірності каналів (U_2), що оцінюється за множиною каналів (показники (U_{2i})); цілісність комплексу засобів захисту, що оцінюється за множиною засобів захисту (показники (U_{3i})); можливість самотестування (U_4), що оцінюється за множиною перевірочних тестів, які наявні в системі (U_{4i}); можливість ідентифікації та автентифікації вузлів при обміні, автентифікації відправника, автентифікації отримувача (U_5), що оцінюється за множиною параметрів оцінки ефективності системи аутентифікації вузлів (U_{5i}).

В схемі моніторингу, що розглядається (див. рис.1), припустимо наявність динамічних зв'язків між її елементами. Сучасна концепція представлення знань в системах штучного інтелекту передбачає наявність змішаної інформації структурованого і неструктурованого типів. На початковому (нульовому) етапі для запропонованої схеми моніторингу формується структура знань системи підтримки прийняття рішень (СППР), що надається підсистемі S_0 підсистемами S_1, S2 .

Розглянемо теперішній момент часу t_0, що відповідає моменту ухвалення рішення та поточному стану системи. Тоді система знань буде включати:

1. Статичні структуровані знання (дані) $D_0(U_i^*,t)$, де $U_i^* \in U^*$– множина граничних значень контрольованих параметрів інформаційної системи; $t \leq t_0$. $D_0(U_i^*,t)$ містить кількісні накопичені знання (дані), які не підлягають подальшій зміні. До таких знань відносяться знання про можливі інциденти системи та стан параметрів системи, що їм відповідає і дозволяє їх визначення.

Така система знань формується на основі метода експертного оцінювання, коли кожному з експертів пропонується визначити характерні для інциденту ознаки в роботі системи та ймовірність їх прояву в окремих випадках. Кожному інциденту відповідає нечітка множина оцінок параметрів, що визначається наступним чином $D_{oi} = \{\mu_{ik} / O_{ik}\}$, де μ_{ik} – визначає ймовірність (можливо нечітку) прояву даної ознаки інциденту O_{ik} .

2. Динамічні структуровані знання (дані) $D_S(t,O_i)$, де $O_i \in W$; $t > t_0$. $D_S(t,O_i)$ містить кількісні прогностичні знання (дані), які можуть коректуватися в процесі роботи. Якщо показники стану об'єктів моніторингу при інциденті не є бінарними, то можливим є наявність якісно різних значень параметра, а його ймовірність розраховується за спрощеною формулою Байєса (3.1):

$$\mu_{ik} = p(N_{ir}|N_i)*p(N_i), \quad (3.1)$$

де $p(N_{ir}|N_i)$ – ймовірність присутності даної ознаки інциденту із r-статусом серед всіх випадків прояву інциденту; $p(N_i)$ – загальна ймовірність прояву ознак відповідного інциденту.

Далі можливим є використання декартового добутку станів системи, що забезпечить наявність декількох альтернативних нечітких множин характеристик прояву інциденту на об'єктах моніторингу кібербезпеки. При формуванні нечіткої множини ознак інциденту, для визначення інцидентів інформаційної системи, включається тільки одне значення, що якісно відповідає поточним параметрам системи.

3. Статичні неструктуровані знання (дані) $D_C(U_i^*,t)$, де $U_i^* \in U^*$; $t \le t_0$. $D_C(U_i^*,t)$ містить базові шкали по різних групах фізичних параметрів, що оцінюються в процесі ухвалення рішень на різних рівнях, спільно із значеннями лінгвістичних змінних, а також накопичені знання (дані), які не підлягають подальшій зміні. Ймовірності прояву ознаки при інциденті визначаються наступним чином: якщо параметри, за якими відбувається моніторинг, мають бінарну оцінку (True або False), то для визначення ваги використовується класичне визначення ймовірності за формулою 3.2

$$j_{ik} = \frac{N_i}{N} \quad . \quad (3.2)$$

Якщо параметри характеризуються діапазоном можливих значень, то

$$\mu_{ik} = \frac{\sum_{i=1}^{n} p_i v_i}{\sum_{i=1}^{n} v_i}, \quad (3.3)$$

де ν_i – ваговий коефіцієнт, що відображує ранг експерта.

4. Динамічні неструктуровані знання $D_L(t,O_i)$, де $O_i \in O$; $t \geq t_0$. $D_L(t,O_i)$ включає прогностичні дані значень лінгвістичних змінних, які можуть коректуватися в процесі роботи. Уточнення коефіцієнту μ_{ik} в процесі роботи системи відбувається шляхом врахування результатів поточного аналізу стану IoT системи і визначення інцидентів, як думки окремого експерту, ранг якого підвищується із збільшенням кількості даних. На етапі тестування роботи системи в базу даних системи управління інцидентами записуються логічні змінні із значеннями всіх параметрів, що підлягають моніторингу. Далі за наявності необхідних даних проводиться аналіз проявів інциденту та призначається додаткове тестування.

Після визначення наявності інциденту та його типу визначаються дії з усунення його проявів. Процес відображення початкової множини знань про інциденти на простір можливих рішень щодо усунення їх проявів і генерацію допустимого рішення здійснюється в підсистемі S_0 . Інтегральна оцінка ймовірності інциденту визначається наступним чином:

$$F_i^k = \sum_{i=1}^{n} M_i D_{oi} + \sum_{j=1, i \neq j}^{B} M_j D_{uj} \,, \qquad (3.4)$$

де $M = \{ \mu_i \}$ – вектор ймовірності прояву ознак при інциденті.

Інтегральна оцінка наявних інформаційній системі ознак інциденту визначається аналогічним чином:

$$F_i^c = M^* D^c \,, \qquad (3.5)$$

де $M^* = \{\mu_i\}$ – розширений вектор ймовірності прояву ознак при інцидентах, в яких за умови наявності в системі ознак, що не належать до ознак даного інциденту, приймаються нульові значення для коефіцієнтів.

Таким чином, в системі враховується можливість одночасного настання двох або більшої кількості інцидентів. Для розрахунку допустимого значення відхилення (ε) з множини еталонних інцидентів необхідно розрахувати граничні інтегральні оцінки за всіма ознаками інцидентів у випадку наявності для кожного інциденту однієї множини ознак або мінімальні та максимальні інтегральні оцінки у випадку наявності альтернативних множин ознак.

Граничними інтегральними оцінками інциденту у випадку наявності для кожного порушення однієї множини ознак інциденту вважається оцінка

співвідношення (3.4), та оцінка, що розраховується за співвідношенням (3.5) лише для підмножини ознак $\mu_{ik}(C_j e_k) \geq \mu^*$ (для достатньої достовірності приймається $\mu^* = 25\%$).

В обох випадках відхилення ε визначається як:

$$\varepsilon = (F_{max} + F_{min})/2 \ . \qquad (3,6)$$

У загальному вигляді система моніторингу має декілька рівнів прийняття рішень. На нульовому рівні здійснюються спостереження, збір, первинна обробка даних, формування системи знань. На першому, другому та третьому рівнях послідовно здійснюється обробка даних з проходженням всіх етапів, передбачених моделлю. Виконання робіт на даних етапах здійснюється системним аналітиком з метою отримання експертної оцінки поточного і прогнозованих станів об'єктів моніторингу. На цих етапах поповнюються динамічні знання системи. На четвертому рівні особа, що приймає рішення, на основі оцінок стану системи, генерує рішення по управляючій дії на об'єкти моніторингу і системи спостереження. Крім того, на даному етапі поповнюється база знань (даних) СППР, вносяться корективи в існуючі знання та відбувається перетворення частини динамічних знань в статичні.

Весь процес управління розглядається в динамічній взаємодії підсистем. У випадку моніторингу інцидентів система може отримати наступні результати:

1. В системі визначено один інцидент інформаційної безпеки, якщо:

а) нечітка множина значень параметрів спостереження в системі відповідає нечіткій множині параметрів спостереження інцидентів *i*-го типу, $E^c = E_i$ або $E^c \in E_i$. Для порівняння множині ознак D_j^c присвоюються значення μ_{ik} , що розраховані для інциденту;

б) інтегральна оцінка множини ознак має відхилення, яке не перевищує певне значення ε , від еталонної множини ознак інциденту, що наявні в базі знань: $\left|F_i^c - F_i^{ek}\right| \leq \varepsilon$.

2. В інформаційній системі одночасно відбуваються декілька інцидентів, якщо:

а) нечітка множина ознак системи перетинається з нечіткою множиною ознак

інформаційних погроз $D_c \cap D$. У такому випадку проводиться пошук сукупності з k інцидентів, що задовольняють умові: $D^c \in \bigcup_{i=1}^{k} D_i$;

б) для кожного типу інцидентів розраховується інтегральна оцінка підмножини ознак D_k^C , що наявні у системі та відповідають певному типу інформаційних погроз з визначеної сукупності, і відхилення від еталонної множини ознак, що наявні в базі знань окремих інцидентів у випадку, коли вони не перевищують певне значення ε для всіх інцидентів: $\left|F_i^c - F_i^{ek}\right| \leq \varepsilon$.

3. Інформаційна система потребує додаткового тестування та моніторингу у випадках, якщо:

а) $E_c \notin E_i$ або $E^c \subseteq \sum_{i=1}^{k} E_i$ та немає можливості змінити масив ознак, виключивши незначні з точки зору кібербезпеки або додавши інші. Тестування визначається у напрямку, що відповідає масиву ймовірних інформаційних загроз: $\inf\{E_c - E_i\}$;

б) $E_c = E_i$ або $E^c = \sum_{i=1}^{k} E_i$, але $\left|F_i^c - F_i^{ek}\right| > \varepsilon$. В такому випадку крім тестування можна визначати дії щодо запобігання або перешкоджання, так як відхилення може бути обумовлене особливостями конкретного інциденту.

4. Знайдено декілька взаємовиключних інцидентів або декілька можливих множин потенційних інформаційних погроз. Тоді найбільш ймовірним є інцидент з найменшим ε . В цьому випадку, за необхідності, можна провести додаткове тестування системи у відповідності до протоколів дій для визначеного переліку інцидентів.

Впровадження підсистеми моніторингу інцидентів реалізованої у відповідності до побудованої моделі дозволяє отримати наступні переваги: вдосконалений моніторинг, що підвищує продуктивність системи; поліпшена інформація для управління якістю обслуговування; виключення втрат і некоректного обліку інцидентів і запитів.

Висновки до третього розділу

1. Проведено аналіз та узагальнення кіберзагроз на компоненти IoT систем результаті якого визначено, що найбільша кількість атак припадає на вузли мережі, а використання безпровідних технологій зв'язку між елементами системи створює передумови для здійснення кібератаки на систему.

2. Визначено, що сьогодні впроваджують багатоступеневі комплексні системи захисту, що базуються на використанні новітніх технічних засобів, кваліфікованих кадрів, контрольних процедурах, адміністративних регламентах з чітким їх дотриманням.

3. Проведемо аналіз атак дозволив визначити їх перелік та дослідити особливості реалізації. В результаті проведеного аналізу і узагальнення розроблено рекомендації з протидії атакам на компоненти IoT системи.

4. Запропоновано модель підсистеми моніторингу інцидентів кібербезпеки в IoT системах. Впровадження підсистеми моніторингу інцидентів реалізованої у відповідності до побудованої моделі дозволяє отримати наступні переваги: вдосконалений моніторинг, що підвищує продуктивність системи; поліпшена інформація для управління якістю обслуговування; виключення втрат і некоректного обліку інцидентів і запитів.

ВИСНОВКИ

В результаті проведеного аналізу фізичних принципів дії засобів виявлення, що використовуються в системах охорони периметру, визначено переваги та недоліки кожного з них, представлено класифікацію систем охорони периметру та класифікацію периметрових засобів виявлення, розглянуті основні типи загороджувальних конструкцій та найбільш відомі системи охорони периметру.

Аналіз мобільних засобів охорони дозволив визначити склад, функціональні особливості такого роду систем. Визначено, що для організації охорони тимчасово розташованих об’єктів можливе впровадження двох груп технічних засобів охорони – відповідно рубіжно-сигналізаційних та розвідувально-сигналізаційних. Визначено, що для проведення процедури ідентифікації особи у швидкорозгортаючих системах охорони периметру необхідним є використання RFID-технологій.

Встановлено, що з метою підвищення рівня захищеності необхідним є удосконалення існуючих моделей та методів побудови швидкорозгортаючих систем охорони периметру шляхом інтеграції переваг вибраних засобів та технологій в єдину систему.

Запропоновано структуру IoT системи охорони периметру, яка включає в себе підсистему безконтактної радіочастотної ідентифікації (RFID) (Модуль 1); підсистему інтелектуального відеоспостереження (Модуль 2); СППР із виявлення та попередження НСД на території об’єкту охорони (Модуль 3); підсистему виявлення руху по контуру периметру захисту (Модуль 4). Інтеграція та реалізація цих підсистем дозволяють автоматизувати процес виявлення порушників та процес прийняття рішень щодо формування сигналу тривоги.

Запропоновано модель взаємодії компонентів IoT системи охорони периметру. Дана модель визначає інформаційні потоки та реалізує взаємодію компонентів системи. Також було визначено форму інформаційних векторів.

Запропоновано метод побудови блоку прийняття рішень з виявлення

несанкціонованого доступу до периметру об’єкту охорони шляхом проектування та налаштування бази знань, що становить собою сукупність лінгвістичних висловів типу ЯКЩО <входи>, ТО <виходи>. Наведені вирази мають форму операцій нечіткої логіки та матриці знань, отже, є можливість автоматизувати процес визначення загроз.

Проведено комп’ютерне моделювання IoT системи охорони периметру засобами Cisco Packet Tracer дозволило перевірити працездатність запропонованих моделей та дозволяє нам визначити потенційні кіберзагрози для даної структури.

Проведено аналіз та узагальнення кіберзагроз на компоненти IoT систем результаті якого визначено, що найбільша кількість атак припадає на вузли мережі, а використання безпровідних технологій зв’язку між елементами системи створює передумови для здійснення кібератаки на систему.

Проведемо аналіз атак на IoT системи дозволив визначити найймовірніші з них та дослідити особливості їх реалізації. В результаті проведеного аналізу і узагальнення розроблено рекомендації з протидії атакам на компоненти запропонованої IoT системи.

Запропоновано модель підсистеми моніторингу інцидентів кібербезпеки в IoT системах. Впровадження підсистеми моніторингу інцидентів реалізованої у відповідності до побудованої моделі дозволяє отримати наступні переваги: вдосконалений моніторинг, що підвищує продуктивність системи; поліпшена інформація для управління якістю обслуговування; виключення втрат і некоректного обліку інцидентів і запитів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Лобанчикова Н.М. Модель побудови мобільної систем охорони периметру території / Н. М. Лобанчикова // Сучасний захист інформації: Наук.-техн. журнал.– Київ: ДУТ, 2020. – №1(41). – С.42 – 48.

2. Лобанчикова Н.М., Серденюк Б.О. Дослідження процесів захисту інформації в IoT. Тези доповідей X Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2019», 18-20 квітня 2019 року. Житомир: ЖДТУ, 2019. С. 80-83

3. Lobanchykova N., Kredentsar S. Methodology for Perimeter Security Systems Creation. Тези доповідей XI Міжнародної науково-технічної конференції «Інформаційно-комп’ютерні технології – 2020 (ІКТ-2020)», 09 - 11 квітня 2020 року. Житомир: Житомирська політехніка, 2020. С.101-102.

4. Юдін О. К. Сучасні практики впровадження системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури / О. К. Юдін, Р. В. Зюбіна, О. В. Матвійчук-Юдіна // Наукоємні технології. – 2019. – № 1. – С. 36-43.

5. Корченко А.Г. Построение систем защиты информации на нечетких множествах [Текст] : Теория и практические решения / А.Г. Корченко. – К. : МК-Пресс, 2006. – 320 с

6. Грайворонський М.В. Безпека інформаційно-комунікаційних систем [Текст] / М.В. Грайворонський, О.М. Новіков – К.:Видавнича група bhv, 2009.– 608 с.

7. Пількевич І. А. Захист інформації в АСУ : навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.

8. Кавун, С. В. Інформаційна безпека: підручник / С. В. Кавун. – Харків: Вид. ХНЕУ, 2009. – 368 с.

9. Белов Е. Основы информационной безопасности : учебное пособие для вузов [Текст] / Белов Е., Лось В., Мещеряков А. – М. : "Студио", 2006. – 356 с.

10. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: [учеб. пособие для вузов]. – М. : Горячая линия-Телеком, 2004. – 280 с.

11. Коцюба В.П. Удосконалення організації охорони тимчасово розташованих військових об’єктів шляхом впровадження сучасних технічних засобів охорони / В.П. Коцюба // Наука і техніка Повітряних Сил : Наук.-техн. журн. – Х.:ХУПС, 2011.– №1(5) – С.164–167.

12. Жуков В.І. Визначення шляхів протидії диверсіям формувань сил спеціальних операцій / В.І.Жуков, В.П. Коцюба, О.С. Тітов // Збірник наукових праць ХУПС. – Х.:ХУПС, 2010. Вип. (4)26. – С. 10-14.

13. Дзеверін І.Г. Синтез структури комплексної системи охорони і оборони військових об’єктів Повітряних Сил / І.Г. Дзеверін І.Л. Костенко, О.М. Борщевський //Наука і техніка Повітряних Сил : Наук.-техн. журн. – Х.:ХУПС, 2010. – Вип. (2)4, – С. 186-190.

14. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345с.

15. SaM Solutions. Структура IoT системи [Електронний ресурс] / SaM Solutions. – 2019. – Режим доступу до ресурсу: https://sam-solutions.by/industries/internet-veschey/

16. Стандарт NB-IoT Low-Power and Wide-Area, LPWA [Електронний ресурс].– 2019. – Режим доступу до ресурсу:
http://www.tadviser.ru/index.php/Статья:Стандарт_NB-IoT_Low-Power_and_Wide-Area,_LPWAN_(Энергоэффективная_сеть_дальнего_радиуса_действия)#.D0.A1.D0.B5.D1.82.D0.B8_LPWAN.

17. Бржевська З.М., Гайдур Г.І., Аносов А.О. Вплив на достовірність інформації як загроза для інформаційного простору / З.М. Бржевська, Г.І. Гайдур, А.О. Аносов // Кібербезпека: освіта, наука, техніка. – 2018. - №2(2). – С. 105-112. (Index Copernicus) DOI: 10.28925/2663-4023.2018.2.105112.

18. Гайдур Г.І. Механізм функціонування цілісної інформаційної системи в умовах кібернетичного впливу [Електронний ресурс] / Г.І. Гайдур, С.О. Гахов // . – Сучасний захист інформації. - №4. – 2019. – С. 22-26 DOI: 10.31673/2409-7292.2019.042226

19. Cisco Packet Tracer [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ua/training-events/netacad/ training-courses/cisco-packet-tracer.html.

20. NetSim Professional [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.tetcos.com/netsim-pro.html

21. Протоколи з'єднання з IoT [Електронний ресурс]. – 2019. – Режим доступу до ресурсу http://www.rtsoft.ru/press/articles/ detail.php?ID=2718.

22. Гнатюк С.Л. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України [Електронний ресурс].– квітень 2019. – Режим доступу https://niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi.

23. Борейко О.Ю. Проектування IoT // електрон. текст. дані URL: https://www.slideshare.net/ssuserf405bc/iot-79608563 (дата звернення: 04.12.2020)

24. Информационная безопасность интернета вещей (Internet of Things) // електрон. текст. дані URL: http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_интернет_вещей_(Internet_of_Things) (дата звернення: 06.12.2020)

25. Богуслав А.М. Методи та моделі забезпечення захисту безпроводних сенсорних мереж// електрон. текст. дані URL: http://er.nau.edu.ua/bitstream/NAU/22464/2/diser_ua_2.0.pdf (дата звернення: 06.12.2020)

26. Орешкина Д. Эталонная архитектура безопасности интернета вещей // Часть 2. електрон. текст. дані URL: https://www.anti- 100 malware.ru/practice/solutions/iot-reference-architecture-protection-part-2 (дата звернення: 04.12.2018)

27. Security in the internet of things // електрон. текст. дані URL: Sehttps://www.windriver.com/whitepapers/security-in-the-internet-ofthings/wr_security-in-the-internet-of-things.pdf (дата звернення: 08.12.2020).

28. John Blyler 8 Critical IoT Security Technologies // електрон. текст. дані URL: https://www.electronicdesign.com/industrial-automation/8-criticaliot-security-technologies (дата звернення: 08.12.2020)

29. Вовк, А.В. Методика забезпечення інформаційної безпеки IoT: магістерська дис.: 172 Телекомунікації та радіотехніка / Вовк Анастасія Віталіївна. - Київ, 2018. - 100 с.

30. Туранска, О.С. Розвиток методів захисту інформації в безпроводових сенсорних мережах: магістерська дис.: 172 Телекомунікації та радіотехніка / Туранська Олена Сергіївна. – Київ: НТУ України «КПІ імені Ігоря Сікорського», 2018. - 67 с.

31. Корченко О. Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах / О.Корченко, М. Алєксандер, Р. Одарченко, А. Наджи, О. Петренко // Захист інформації, 2016. – № 1. – С. 48-56.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)