

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

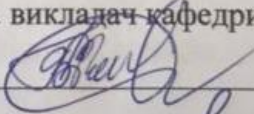
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи охорони периметру
приватного домоволодіння»

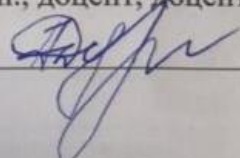
Виконала студентка 4-го курсу, групи ЗКБ-17
спеціальності 125 «Кібербезпека»

 Вікторія ЛОБАНЧИКОВА

Керівник ст. викладач кафедри КН

 Віталій ЛЕВКІВСЬКИЙ

Рецензент к.т.н., доцент, доцент кафедри БІтаТ

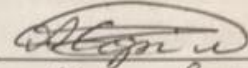
 Олександр ДУБИНА

Житомир – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «Кібербезпека»

ЗАТВЕРДЖУЮ

зав. кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО
« 12 » квітня 20 21 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студентки Лобанчикової Вікторії Сергіївни

Тема роботи: Проект системи охорони периметру приватного домоволодіння

Затверджена наказом університету від « 12 » квітня 2021 р. № 134/С

Термін здачі студентом закінченої роботи: « 20 » серпня 2021 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження): схема домоволодіння; план будинку; час роботи системи: постійно; стійкість до зовнішнього природного середовища; можливість отримання сповіщення на телефон, зняття сигналізації засобами RFID; робочий діапазон температур: -25⁰С до +35⁰С, можливість перегляду стану системи через Інтернет. Об'єктом дослідження виступають технології побудови систем охорони периметру та їх захист. Предметом дослідження є моделі, методи та засоби побудови систем охорони периметру домоволодіння.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

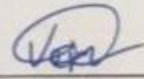
Керівник

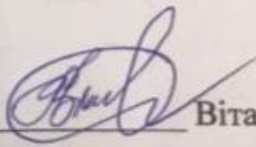


Віталій ЛЕВКІВСЬКИЙ

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	12.04.21	виконано
2	Аналіз завдання та дослідження предметної області, уточнення завдання	14.04.21 – 18.04.21	виконано
3	Аналіз літературних джерел та написання розділу 1	19.04.21 – 20.04.21	виконано
4	Розробка проекту системи, формування розділу 2	24.04.21	виконано
5	Розробка алгоритму роботи системи	27.04.21 – 29.05.21	виконано
6	Комп'ютерне моделювання та розробка програми функціонування	01.06.21 – 04.06.21	виконано
7.	Тестування програми, формування розділу 3	05.6.2021-08.06.2021	виконано
8.	Доопрацювання пояснювальної записки	08.06.2021-10.06.2021	виконано
9.	Підготовка графічного матеріалу	10.06.2021-14.06.2021	виконано
7	Проведення попереднього захисту	15.06.21	виконано
8	Отримання відгуку керівника	16.06.21	виконано
9	Допуск завідувача кафедри	17.06.21	виконано
10	Подання роботи на рецензування	18.06.21	виконано
11	Захист	Згідно розкладу	виконано

Студентка  Вікторія ЛОБАНЧИКОВА

Керівник  Віталій ЛЕВКІВСЬКИЙ

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи викладена на 74 сторінках, містить 49 рисунків, 2 таблиці та 2 додатки, що розміщено на 10 сторінках. Перелік джерел посилання містить 28 літературних джерел і займає 3 сторінки. Загальний обсяг роботи складає 84 сторінок.

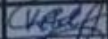
Метою кваліфікаційної роботи є розробка проєкту системи охорони периметру приватного домоволодіння для підвищення рівня захищеності майна від несанкціонованого доступу з відповідним рівнем кіберзахисту.

Об'єктом дослідження виступають технології побудови систем охорони периметру та їх захист.

Предметом дослідження є моделі, методи та засоби побудови захищених систем охорони периметру домоволодіння.

У першому розділі кваліфікаційної роботи представлено теоретичні аспекти побудови систем охорони периметру, аналіз аналогів та базові технології. Другий розділ присвячено розробці проєкту системи охорони периметру домоволодіння, здійснено аналіз об'єкту охорони, розроблено структуру системи, запропоновано функціональну модель системи, здійснено вибір обладнання та розроблено електричну принципову схему щита управління. Третій розділ присвячено розробці блок-схеми алгоритму роботи системи та програмній реалізації. Розроблена система охорони периметру домоволодіння закінчена, готова до використання, може бути встановлена на об'єкті дослідження. Перспективним є розробка Веб-орієнтованої системи для власника домоволодіння та дослідження процесів інтеграції систем охорони з даним Веб-додатком.

Ключові слова: ДОМОВОЛОДІННЯ, МОДЕЛЬ, ОХОРОНА, ПЕРИМЕТР, СИГНАЛІЗАЦІЯ, СИСТЕМА.

					КБ.КР.Б – 125 – 08 – ПЗ			
Зм	Арк.	№ докум.	Підпис	Дата	Проект системи охорони периметру приватного домоволодіння Пояснювальна записка	Літ.	Арк.	Аркуші
Розроб.		Лобанчикова В.		30.06.21				
Керівник		Левківський В.Л.		30.06.21			3	84
Рецензент		Дубина О.Ф.		30.06.21		Житомирська політехніка, ФІКТ, група ЗКБ-17		
Н. контр.		Левківський В.Л.		30.06.21				
Зав. каф.		Сфіменко А.А.		30.06.21				

ABSTRACT

The bachelor's thesis is devoted to the development of a project for the protection of the perimeter of a private household to increase the level of protection of property from unauthorized access with the appropriate level of cyber security.

The developed system corresponds to the modern development of science and technology, construction using modern equipment.

Development and testing of the program of operation of the home perimeter security system, the essence of which is the management of the system of protection of premises from unauthorized access based on the MaxyConFlexy controller using a special software environment in the controller emulator "FBD Configurator".

Computer simulation tools simulated the operation of the designed system, which checked the functionality and correct operation of the program for the controller MaxyConFlexy, written in the graphic programming language FBD (Function Block Diagram), which is standardized by the international standard IEC 61131-3.

The explanatory note to the bachelor's thesis contains 85 pages, 49 figures, 2 tables, 2 appendices and 28 references.

Key words: HOUSEHOLD OWNERSHIP, MODEL, SECURITY, PERIMETER, SIGNALING, SYSTEM.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		4

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	6
ВСТУП	7
1 АНАЛІЗ МЕТОДІВ, ЗАСОБІВ ТА ТЕХНОЛОГІЙ СИСТЕМ ОХОРОНИ ПЕРИМЕТРУ	9
1.1 Аналіз сучасних систем охорони периметру	9
1.2 Аналіз засобів виявлення в системах охорони периметру	16
1.3 Аналіз проблеми забезпечення кібербезпеки компонентів IoT систем	21
Висновки до розділу 1	26
2 РОЗРОБКА ПРОЕКТУ СИСТЕМИ ОХОРОНИ ПЕРИМЕТРУ ПРИВАТНОГО ДОМОВОЛОДІННЯ	27
2.1.Аналіз розміщення домоволодіння	27
2.2.Функціональна модель системи охорони периметру домоволодіння.	28
2.3.Вибір обладнання для функціонування системи	31
Висновки до розділу 2	44
3. РОЗРОБКА БЛОК-СХЕМИ АЛГОРИТМУ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ	45
3.1. Розробка блок-схеми алгоритму.....	45
3.2. Розробка програми для роботи контролера	47
3.3. Тестування системи	54
3.4. Аналіз кіберзагроз компонентів системи при реалізації на базі IoT.....	57
Висновки до розділу 3	68
ВИСНОВКИ.....	69
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	71
ДОДАТКИ.....	74

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРМ – Автоматизоване робоче місце.

RFID – Radio Frequency Identification.

ДБЖ – джерело безперебійного живлення

ІЧ – інфрачервоний

ЛВХ – лінії витікаючої хвилі

НСД – несанкціонований доступ

СКУД – Система контролю і управління доступом

ТЗО – технічні засоби охорони.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						6
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Розвиток інформаційних технологій дає нові можливості для суспільства. Сучасні технології заповнили наше життя. «Діджиталізація», «IoT», «кібербезпека» стали невід’ємною частиною спілкування сучасного цифрового суспільства. Важко уявити своє життя без технологій мобільного зв’язку, засобів автоматизації, гаджетів, побутових приладів та іншої техніки. Перехід суспільства у цифровий простір створює сприятливі умови для нашого життя, однак, слід зазначити, що цифровізація суспільства створює передумови виникнення все нових і нових кіберзагроз, що вимагає ретельної уваги фахівців та професіоналів з кібербезпеки та сучасного IT-фахівця при побудові будь-яких систем та впровадженні технологій.

Тому побудова сучасних захищених автоматизованих та інформаційних систем є актуальною задачею сьогодення.

Зростання вартості матеріальних цінностей та кількості крадіжок, вандалізму, злочинів призводять до бажання захисту свого майна особами. Сучасний ринок надає широкий вибір засобів для охорони об’єктів від несанкціонованого доступу (НСД) та охорони периметру території. Системи керування і управління доступом (СКУД) стали невід’ємною частиною організації бізнесу та швидкими темпами проваджуються у захист особистого майна. Особливо актуальною є створення сучасних систем охорони периметру приватного домоволодіння. Робота такого роду систем дуже часто проводиться у «польових» умовах, при складних умовах зовнішнього середовища та у віддаленій місцевості, тому високими є вимоги до надійності складових такого роду систем. Крім того, слід зазначити, що власники домоволодінь при встановленні систем охорони периметру хочуть мати постійний моніторинг стану системи і можливість дистанційного (віддаленого) управління, використання IoT-технологій та IoT-систем, безпроводних технологій, що передбачає підключення системи до мережі, у тому числі Інтернет, що створює передумови виникнення кіберзагроз та вимагає додаткових параметрів стійкості

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

до кібератак різної направленості. Створення захищених систем охорони периметру є актуальною задачею сьогодення.

Метою кваліфікаційної роботи є розробка проєкту системи охорони периметру приватного домоволодіння для підвищення рівня захищеності майна від несанкціонованого доступу з відповідним рівнем кіберзахисту.

Об’єктом дослідження виступають технології побудови систем охорони периметру та їх захист.

Предметом дослідження є моделі, методи та засоби побудови захищених систем охорони периметру домоволодіння.

Для досягнення зазначеної мети необхідним є вирішення наступних взаємозалежних інженерно-технічних *задач*:

- провести аналіз систем охорони периметру;
- провести аналіз технологій побудови систем охорони периметру;
- провести аналіз кіберзагроз, притаманних системах охорони периметру;
- розробити проєкт системи охорони периметру приватного домоволодіння;
- провести реалізацію програмного забезпечення роботи контролера;
- провести перевірку працездатності спроектованої системи засобами комп’ютерного моделювання;
- розробити рекомендації щодо кіберзахисту даної системи.

Методологія роботи – системний аналіз, методи об’єктно-орієнтованого проектування та моделювання, методи комп’ютерного моделювання.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		8

1 АНАЛІЗ МЕТОДІВ, ЗАСОБІВ ТА ТЕХНОЛОГІЙ СИСТЕМ ОХОРОНИ ПЕРИМЕТРУ

1.1 Аналіз сучасних систем охорони периметру

Проведемо аналіз систем охорони периметру, що представлені сьогодні на ринку. Система охорони периметра спрацює при спробі порушника перетнути зовнішній фізичний або умовний кордон. Якщо людина опиниться в зоні виявлення датчика охорони периметру, сигналізація сповістить про це зацікавлену особу.

Є ряд правил для якісного та належного встановлення датчиків систем охорони периметру. Вуличні датчики периметра встановлюються уздовж зовнішньої межі ділянки під охороною. Детектори розміщуються на огорожі, а за її відсутності – на штативах безпосередньо на території. Кожен сповіщувач «відповідає» за вузьку прямолінійну зону певної протяжності. Пристрої підключаються до центрального блоку сигналізації, який обробляє сигнали, що надходять по кабелю або радіоканалу. При спрацьовуванні датчика централь реагує відповідним чином – вмикає сирену, сповіщає користувачів (смс, дзвон), передає сигнал тривоги на пульт охорони.

Перший зовнішній рубіж охорони створюється за допомогою вуличних датчиків периметра різних типів [1-11]:

- активних ІЧ-бар'єрів;
- пасивних ІЧ-детекторів;
- ємнісних датчиків;
- радіопроменевих сповіщувачів.

У системах безпеки приватних будинків найчастіше використовуються активні ІЧ-датчики, які ефективні на відносно прямих ділянках без кущів, колючого дроту та інших перешкод. Радіохвильові моделі мають велику зону виявлення, завдяки чому використовуються на великих промислових об'єктах. Ємнісні датчики підходять для територій зі складним нерівномірним рельєфом,

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

а пасивні інфрачервоні детектори – для охорони невеликих ділянок (наприклад, воріт двору).

Для коректної роботи радіохвильових датчиків необхідно уздовж периметра створити «зону відчуження» – вільний від рослинності простір шириною 1,5–2 метри. Активні інфрачервоні детектори в такій території не потребують.

Активні променеві інфрачервоні датчики створюють вузький бар'єр висотою від 60 см до 3 м. Бар'єр складається з 2–10 променів – в залежності від кількості променевих модулів. Чим більше променів – тим вище, а, отже, надійніше захисна «стіна».

Охоронна зона формується приймачем (фотоприймальним блоком, трансмітером) і передавачем (ресивером), які встановлюються один навпроти одного. Діоди приймача випромінюють ІЧ-пучки світла, а діоди ресивера приймають їх. Сигналізація периметра спрацьовує при перекритті людиною двох або більше променів.

При виборі активного ІЧ-бар'єру слід звернути увагу на наступні характеристики:

- довжина променя – 50–200 метрів, різні показники для приміщення (більше) і вулиці (менше);
- горизонтальний і вертикальний кут;
- тип підключення – дротове, бездротове;
- ступінь захисту від вологи і пилу – для вулиці не менше IP64;
- діапазон температур – від -25–30 до +5–60 °С (для суворих зим можна придбати нагрівачі, які встановлюються всередині корпусів приймача і передавача);
- можливість регулювання чутливості.

Серед доступних систем охорони можна виділити наступні три класи:

1. Дротові системи.
2. Бездротові системи.
3. GSM-сигналізації.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

На ринку України бездротові системи охорони представлені наступні рішення від компаній: ATIS, Ajax Systems, Pyronix, Eldes, Hikvision, MAKС Pro, РифРинг, Elmes Electronics, Satel MICRA та ін.

Простий монтаж і «мобільність» – переваги бездротової сигналізації. Встановлення займає 2–3 години і може проводитися в приміщеннях з чистовою обробкою. При переїзді обладнання можна легко демонтувати, а потім зібрати в новому місці.



Рисунок 1.1 – Стандартна комплектація безпроводної системи

У стандартну комплектацію бездротової сигналізації входить централь (з вбудованою клавіатурою і без неї), сирена, датчики (відчинення дверей, руху), блок живлення і радіобрелоки для постановки/зняття на охорону, рис. 1.1.

Сигналізація масштабується за допомогою додаткових сенсорів [1]:

- магнітно-герконовий – відчинення дверей/вікон;
- акустичних – розбиття;
- інфрачервоного або мікрохвильового – руху;
- побутових – затоплення, диму, витоку газу.

Детектор, що спрацював передає сигнал на центральний блок по радіоканалу (частота 315, 433 або 868 МГц). Після його обробки вмикається сирена і активується функція оповіщення.

Стандартний алгоритм дій – відправка тривожних SMS і/або послідовний дзвінок за вказаними номерами телефонів і на пульта охорони. Деякі моделі сигналізують про зміну режиму роботи або вимкнення електрики. Для оповіщення використовується SIM-карта, яка вставляється в слот GSM-модуля.

Центральний блок підключається до мережі через адаптер (12В). У разі вимкнення електрики використовується вбудований резервний акумулятор, ємності якого вистачає в середньому на 4–12 годин автономної роботи. Для збільшення цього показника варто оснастити систему окремим додатковим блоком живлення (ДБЖ).

Датчики отримують живлення від стандартних батарейок, які можуть служити від декількох місяців до 2–3 років (в залежності від типу). Система контролює електроживлення всіх компонентів і інформує користувача про виникаючі проблеми за допомогою SMS.

Будь-яка бездротова GSM-сигналізація підтримує кілька способів керування [1]. Користувач може вмикати і вимикати режим охорони за допомогою клавіатури, радіобрелка або мобільного телефону. В останньому випадку використовуються SMS-команди, DTMF-коди (введення цифр) або спеціальні додатки (за наявності у централі модуля Wi-Fi). Налаштування зручніше проводити за допомогою клавіатури з дисплеєм, на якому відображається інформація про всі вжиті команди.

Бездротові датчики «прив'язуються» до охоронних зон. Їх кількість залежить від моделі сигналізації і становить від 10 до 122. Подібне розділення дозволяє визначати місцезнаходження і типи сенсорів, що спрацювали. В одній зоні можна зареєструвати кілька детекторів.

У деяких випадках комплектні сенсори за замовчуванням прописані в певних осередках пам'яті (геркон – перша зона, датчик руху – друга зона та ін.). В цьому випадку користувачеві не доводиться займатися реєстрацією, що значно спрощує процес налаштування.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		12

Зоні можна призначити назву («передпокій», «гараж», «вітальня») і задати алгоритм роботи. Більшість систем підтримує кілька режимів, в числі яких – загальна охорона (при ввімкненні відбувається активація, при вимкненні – деактивація), часткова охорона (можна ввімкнути або вимкнути окремо) і постійна охорона (для датчиків задимлення, затоплення, витоку газу).

Додаткові функції [1]:

- Wi-Fi модуль – забезпечує передачу тривожних push-повідомлень через інтернет, дозволяє керувати системою за допомогою програми;
- таймер – дозволяє автоматизувати вмикати або вимикати режими охорони, встановивши необхідний час;
- другий слот для SIM-карти – дозволяє використовувати додаткову сімку, яка активується при поганому прийомі сигналу;
- затримка ввімкнення/вимкнення – бездротова сигналізація з датчиком руху ставиться або знімається з охорони через 10–99 секунд після активації режиму, що запобігає помилковим спрацюванням;
- двосторонній зв'язок – вбудовані мікрофон і динамік дозволяють використовувати централь GSM-сигналізації в якості телефону (в режимі інтерком);
- контроль електроживлення – відправка SMS-повідомлень при виникненні проблеми (вимкнулася електрика, сіла батарея);
- контроль стану – SMS-звіт під час кожної зміни режиму роботи;
- релейний вихід – до контактів реле підключаються електроприлади.

Етапи монтажу:

1. Встановлення центрального блоку з активованою SIM-картою.
2. Кріплення датчиків на входних дверях (герконів), вікнах (розбиття скла), стінах (руху).
3. Налаштування сигналізації за допомогою мобільного телефону або клавіатури, «прив'язка» датчиків до охоронних зон.

Сучасний GSM комплект – це простий, зручний у використанні і надійний варіант сигналізації, який вбереже будинок або квартиру від спроби

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		13

проникнення зломисників. Особливість таких систем – наявність модуля GSM, який дозволяє відправляти SMS-повідомлення і здійснювати голосові дзвінки при тривожних подіях, рис.1.2. На рисунку 1.3 представлено повний комплект безпроводної GSM-системи Kerui PG500. При цьому функціональні можливості комплекту GSM-сигналізації різних моделей можуть відрізнятися. Одні пристрої підтримують тільки оповіщення користувача через дзвінки або повідомлення, іншими можна дистанційно керувати через спеціальне мобільний застосунок.



Рисунок 1.2 – Вигляд GSM-системи



Рисунок 1.3 – Повний комплект безпроводної GSM-системи Kerui PG500

Незаперечна гідність систем цього типу – відсутність істотних обмежень по відстані. Для зв'язку досить, щоб смартфон користувача залишався в зоні покриття мобільного мережі.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		14

Залежно від типу підключення, представлені на ринку комплекти GSM-систем охоронної сигналізації діляться на дві категорії:

- бездротові;
- дротові.

Системи бездротового типу більш зручні у встановленні і експлуатації, оскільки дозволяють швидко організувати контроль над об'єктом, що охороняється. Для цього датчики, блоки та інші елементи системи безпеки розставляються в потрібних місцях: входні двері, вікна та ін. Залежно від моделі радіус дії бездротового сигналу знаходиться в межах 20-300 метрів.

Елементи дротової системи з'єднуються один з одним за допомогою сигнального кабелю, який вкрай бажано захвати – монтувати всередину стіни або за спеціальними коробами. Подібне ускладнює процес монтажу, тому встановлення таких пристроїв важливо враховувати при проектуванні або ремонті приміщення. В іншому випадку зловмисникам буде простіше виявити і знешкодити систему сигналізації.

Важливе значення для будь-якої системи має кількість обслуговуваних зон безпеки. Ця характеристика безпосередньо пов'язана з кількістю і типом комплектних датчиків, площею території, що охороняється.

Так, найпростіші пристрої комплектуються набором з 1-2 датчиків, які користувач розміщує на дверях, вікнах, стінах і інших елементах всередині приміщення. Такі дозволяють організувати охорону гаражів і невеликих квартир.

Якщо ж потрібна система для великих площ, краще придивитися до моделей на 30 і більше незалежних зон. Ціна на подібні системи вище, але вони комплектуються датчиками відчинення дверей, розбиття вікон, задимлення. Купити комплект GSM сигналізації цього типу варто для багатокімнатної квартири або приватного будинку.

Приклад системи охорони периметру представлено на рисунку 1.4. Слід зазначити, що «периметром» у такому випадку вважається межа території, що знаходиться під захистом. Ця межа є найкращим місцем для раннього детектування вторгнення порушника.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.4 – Система охорони периметру домоволодіння

Особливості проєктування системи охорони периметра полягають у тому, що охоронні датчики встановлюються на різноманітних конструкціях та перекривають досить великі ділянки.

1.2 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 систем охорони периметру 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.

Основна задача систем охорони периметру полягає в цілодобовому контролі периметру від несанкційованого проникнення на територію або виходу за територію даного об'єкту. Периметрова межа об'єкта є найкращим місцем для раннього детектування вторгнення, тому що порушник взаємодіє в першу чергу

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		16

з фізичним периметром і створює коливання, які можна зареєструвати спеціальними датчиками.

Практично всі дії порушника дають можливість для електронного виявлення, тому що створюють певний рівень вібрацій і специфічний звуковий “образ” вторгнення. При певних умовах порушник може уникнути фізичного контакту з периметром. В цьому випадку можна використовувати «об’ємні» датчики вторгнення, зазвичай грають роль вторинної лінії захисту. Тому для вибору системи охорони периметру підходять комплексно. Залежно від принципу дії системи охорони периметру можуть захищати:

- тільки периметри, мають загородження (паркани);
- тільки периметри, що не мають загородження.

На вибір типу периметрової сигналізації в першу чергу впливає її стійкість до дії зовнішніх кліматичних чинників, які можуть бути присутніми на об’єкті, що охороняється. Вибір конкретних типів периметрових систем охоронної сигналізації проводиться в залежності від: наявності та виду огорожі (цегляний паркан, сітка і т.д.); наявності смуги відчуження та її ширини; протяжності периметра; рельєфу місцевості.

Інфрачервоні системи діляться на два типи: активні та пасивні, рис. 1.5. Активні периметричні системи – це передавач-випромінювач кілька лінійних невидимих променів і приймач. Пасивні системи працюють за принципом виявлення теплового випромінювання від рухомого об’єкту в зоні виявлення. Залежно від лінзи датчика зони можуть мати або лінійний вид, або мати об’ємні характеристики.

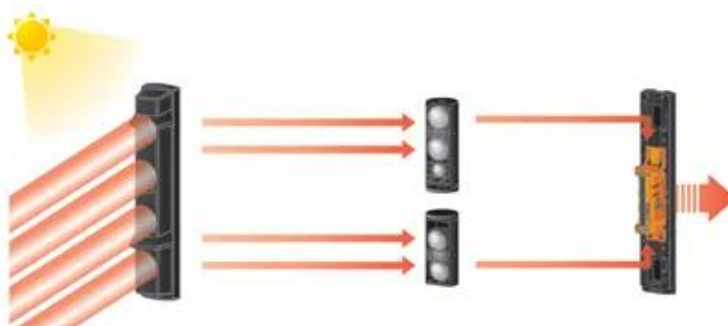


Рисунок 1.5 – Інфрачервоні системи

Провідно-хвильові сповіщувачі, рис. 1.6. Принцип дії заснований на створенні в просторі електромагнітного поля уздовж відкритої провідної лінії, що розташовується на рубежі охорони, і реєстрації зміни цього поля при перетині його порушником. Всі типи виробів мають дистанційний контроль працездатності, грозозахист зовнішніх ланцюгів. Об'ємна зона виявлення формується «відкритою антеною» – двома паралельно розташованими проводами (кабелями), до яких відповідно підключаються генератор УКХ-діапазону і приймач. Зона виявлення може бути як «козиркового», так і «приземного» типу, рис.1.6.

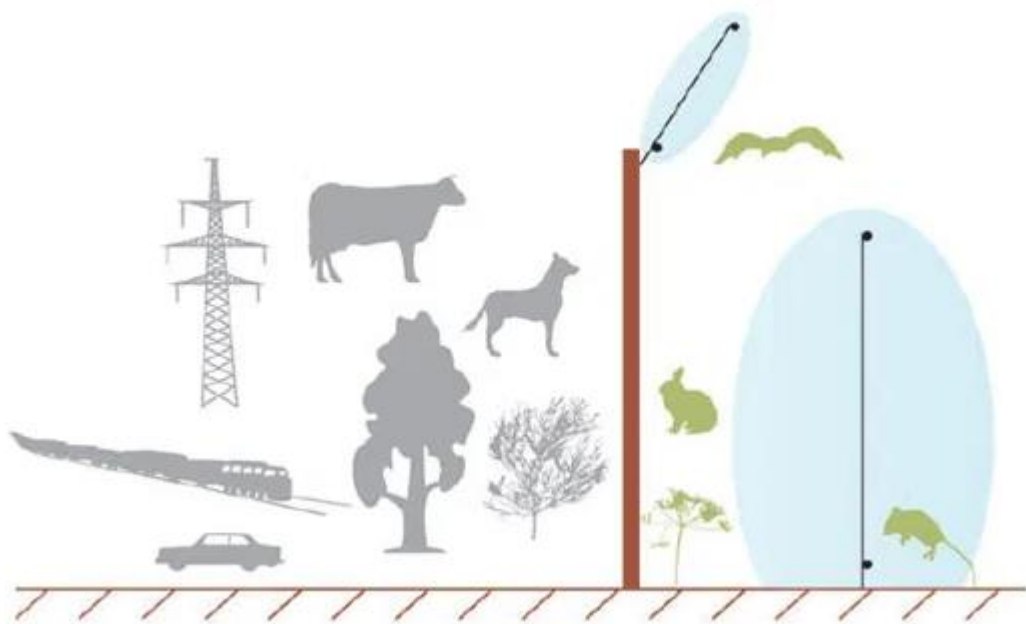


Рисунок 1.6 – Провідно-хвильові сповіщувачі

Підземні сенсорні кабелі, рис. 1.7. В системі використовуються сейсмічні сенсори, які реєструють коливання або стиснення ґрунту уздовж периметра. Підземна установка датчиків забезпечує їх ефективне маскування, роблячи сенсори практично невидимими для потенційного порушника. Вмонтовані в ґрунті датчики дозволяють захищати периметри, на яких установка традиційних «наземних» охоронних датчиків є неможливою в силу природно-кліматичних (схили гір, береги річок, лісові масиви і т.п.) або естетичних умов (музейні комплекси, пам'ятники архітектури, історичні об'єкти).

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18



Рисунок 1.7 – Вигляд встановлення сенсорних кабелів

Ємнісні системи охорони периметра, рис.1.8 використовують ефект зміни характеристик електричного поля при наближенні або дотику порушника до огорожі об'єкта.



Рисунок 1.8 – Вигляд ємнісних систем охорони

Використовуються електроди, які кріпляться до жорсткої огорожі на ізоляторах. Це свого роду антени, призначені для поширення і вимірювання ємності електричного сигналу, який створюється електронним блоком.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

Наближення до них, дотик змінює ємність електричного поля, що і є приводом для подачі тривожного сигналу.

Під час проектування системи потрібно враховувати:

- довжину периметру, що впливає в першу чергу на вибір станції управління та типи сповіщувачів;
- знати особливості рельєфу території та розміщення будівель;
- який тип огорожі використовується на периметрі;
- ймовірні місця порушення;
- кліматичну зону даного об'єкту;
- враховувати те, що дана система буде працювати цілодобово;
- кому і яким чином будуть передаватися сигнал про порушення;
- які потрібно формувати сигнали керування при тій чи іншій ситуації на об'єкті;
- час реагування на сигнал порушення;
- та багато інших факторів, які будуть впливати на якість та продуктивність самої системи.

В наш час ринок дає широкий спектр інженерно-технічних систем охорони периметру з різноманітними новітніми технологіями, які дають можливість створити сучасну систему з високою ймовірністю виявлення порушень периметру та зменшити кількість неправдивих тривог. 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.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		20

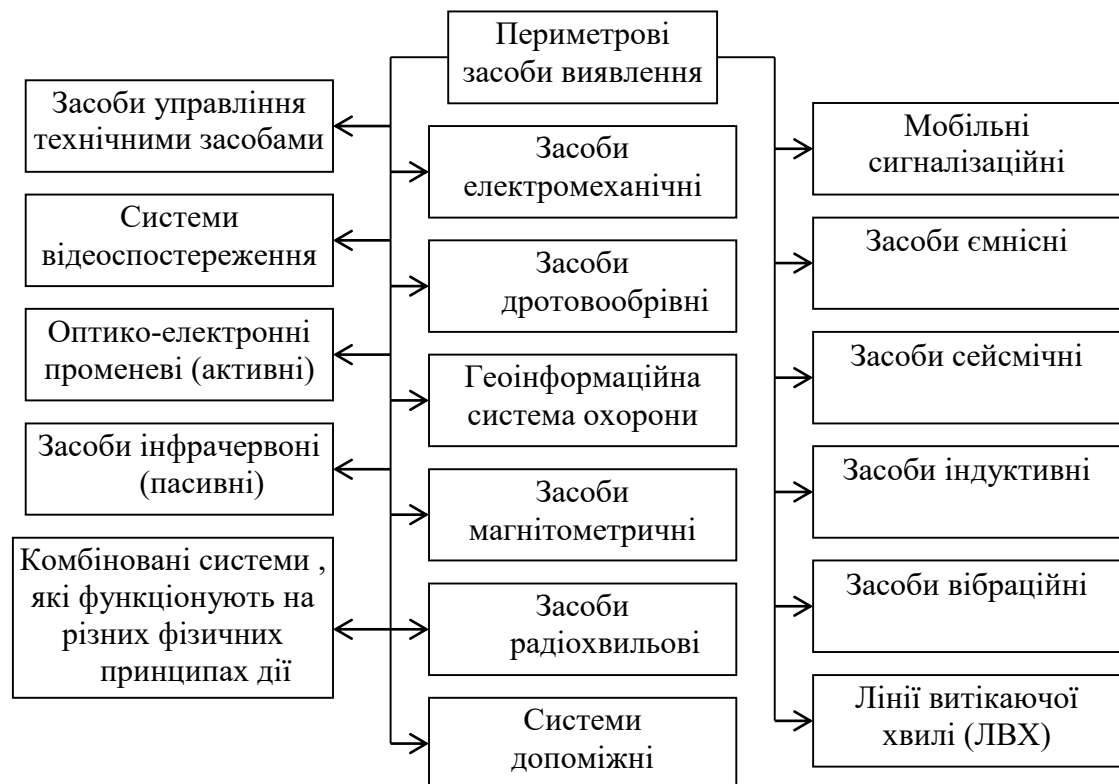


Рисунок 1.9 – Класифікація периметрових засобів виявлення за їх фізичними принципами дії

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.

1.3 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 [12-18]. 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 [19]: 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-інтерфейс 60% пристроїв експерти HP вважають небезпечним через недосконалу організацію доступу і високий ризик міжсайтового скриптингу. У більшості

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		22

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 [19-28]: 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 1.10 продемонстроване середовище безпеки, пов'язане з логічною структурою IoT.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

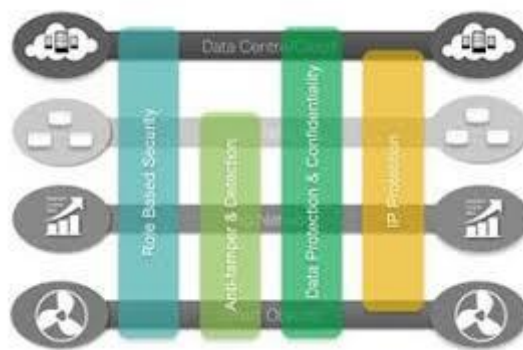


Рисунок 1.10 – Середовище безпеки IoT

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 рівні архітектури.

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

На рисунку 1.10 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.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

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 розділу 1

1. В результаті проведеного аналізу систем охорони периметру визначено, що є три класи систем, а саме дротові, бездротові та GSM-сигналізації.

2. Комплектація систем, що представлені на ринку є типовими. Всі сигналізації масштабується за допомогою додаткових сенсорів.

3. Проведено аналіз та узагальнення кіберзагроз на компоненти IoT систем результаті якого визначено, що найбільша кількість атак припадає на вузли мережі, а використання безпроводних технологій зв'язку між елементами системи створює передумови для здійснення кібератаки на систему. Таким чином провідні системи мають більшу стійкість до зламу.

4. 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.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						26
Змн.	Арк.	№ докум.	Підпис	Дата		

2 РОЗРОБКА ПРОЕКТУ СИСТЕМИ ОХОРОНИ ПЕРИМЕТРУ ПРИВАТНОГО ДОМОВОЛОДІННЯ

2.1. Аналіз розміщення домоволодіння

Об'єкт представляє собою невеличке домоволодіння, рис. 2.1.

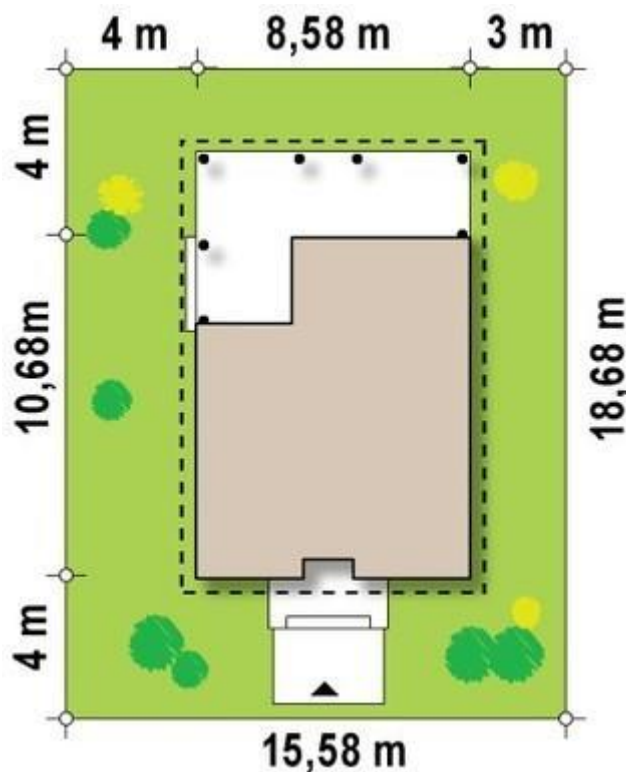


Рисунок 2.1. – Загальний вигляд домоволодіння

Об'єкт розташований на прямокутній ділянці. Будинок розміщено посередині ділянки. Ділянка розташована у селищі, де зліва, праворуч неї є інші будинки та присадибні ділянки. Попереду знаходиться дорога, за якою розміщено присадибну ділянку з будинком. Позаду до ділянки примикає озеро.

План будинку представлено на рис. 2.2. Загальна площа забудови 113,42 м². Будинок містить відкриту терасу, площею 30,9 м², дві дитячі кімнати, 10 м² та 9,7 м², кухню-столову, загальною площею 22,4 м², спальнею, 9,2 м², вхідною групою (тамбур) 2,1 м², коридор 6 м², санвузол, площею 3,7 м² та технічне приміщення, 2,3 м².

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		27

Будинок побудовано з піноблоку, утеплення здійснено ековатою, зовні стіни оздоблено структурною штукатуркою. Стінні перегородки всередині виконані з гіпсокартону.

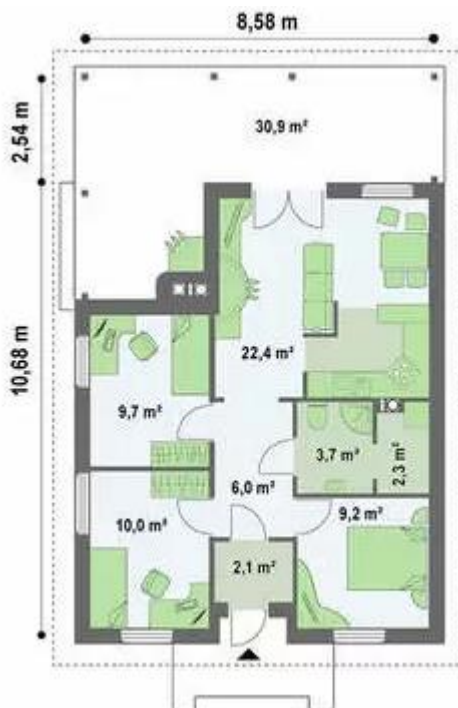


Рисунок 2.2 – План будинку

Переkritтя та стеля виконані з дерева, для оздоблення стелі використано натяжні полотна, що опущені на 20 см. Вікна в офісних приміщеннях – пластикові зі склопакетами. З внутрішньої сторони обладнані жалюзіями з тканини. Вхідні двері в приміщення одностулкові 90x200 см, пластикові з врізаним механічним замком.

2.2. Функціональна модель системи охорони периметру домоволодіння

Опираючись на результати проведеного аналізу пропонується наступна структурна схема системи охорони периметру домоволодіння. До складу системи входять наступні модулі: модуль сповіщувачів, модуль виконавчих механізмів, модуль безперебійного живлення, підсистема управління доступу та охорони об'єкту, рис. 2.3.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		28

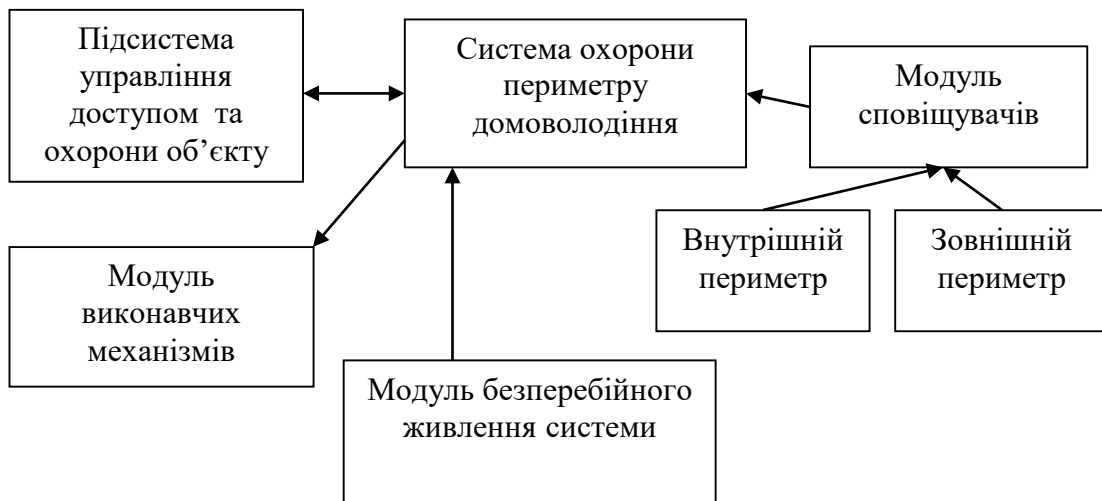


Рисунок 2.3 – Структурна схема системи

Модуль виконавчих механізмів представлено світловою індикацією стану системи та звуковим сигналом (сигнальна сирена). Модуль безперебійного живлення потрібен для гарантованого живлення системи (щоб система знаходилась у працездатному стані) і розрахований на 24 години безперебійної роботи. Модуль сповіщувачів представляє собою набір сповіщувачів для здійснення контролю за внутрішнім периметром та набір сповіщувачів для контролю за зовнішнім периметром домоволодіння. Набір давачів внутрішнього периметру складають: герконові датчики для контролю за положенням дверей та віконних блоків, датчики руху. Набір давачів зовнішнього периметру складають давачі руху, що розміщено по «контур» будинку, інфрачервоний бар'єр по периметру ділянки для виявлення вторгнень на територію домоволодіння.

Підсистема управління доступом та охорони об'єкту являє собою набір компонентів для здійснення моніторингу за станом датчиків, прийняття рішень та управління виконавчими механізмами, а також здійснення передачі сигналів на веб-сервер.

Для поставленої задачі можна вибрати готове рішення, однак прийомо-контролюючих пристрій, що представлений на ринку не дає можливості провести програмну реалізацію та перевірити правильність проєктних рішень. Тому для реалізації даної системи та перевірки правильності прийнятих рішень

використаємо вільнопрограмований контролер українського виробника РАУТ-автоматік та їх програмне забезпечення для комп'ютерного моделювання.

В результаті проведених досліджень та на підставі розробленої структурної схеми функціональних модулів проводимо розробку функціональної схеми. Функціональна схема системи представлена на рисунку 2.4.

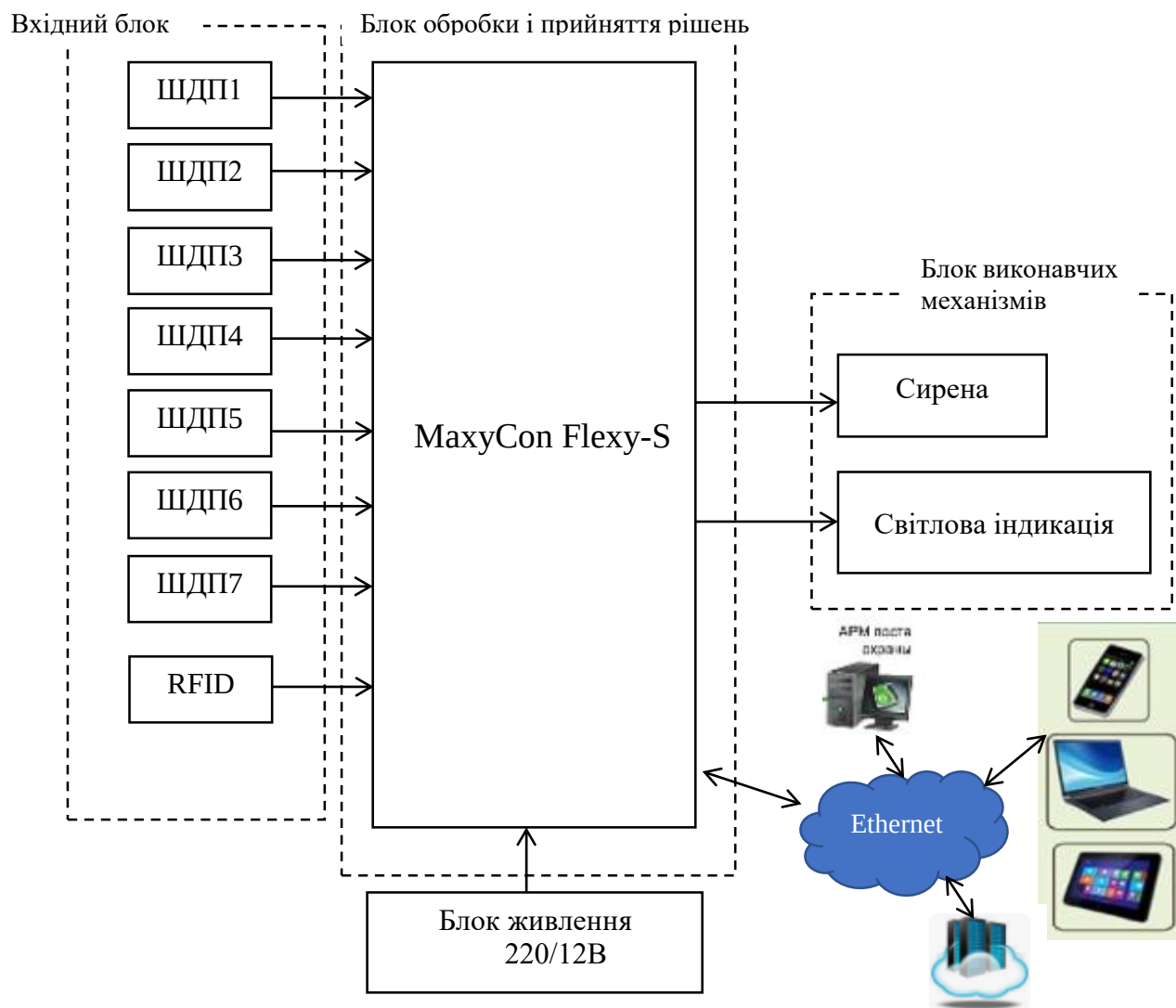


Рисунок 2.4 – Функціональна схема системи охорони периметру домоволодіння

Як видно, з рисунку 2.4, система складається з трьох основних блоків: вхідного блоку, блоку обробки інформації та прийняття рішень, а також блоку виконавчих механізмів. Блок обробки інформації та прийняття рішень підключено до мережі Інтернет, що дає можливість відправляти всі дані з контролеру на веб-сервер, АРМ поста охорони, гаджети власників домоволодіння.

Вхідний блок включає в себе підключення шлейфів датчиків приміщень (ШДП1-ШДП7) та імпульсного сигналу від підсистеми RFID. Технології RFID використовуються для зняття та встановлення системи на «охорону». Власне дана підсистема містить зчитувач RFID-міток, контролер для перевірки правильності коду та подачі команди на встановлення/зняття з режиму «охорона». На блок обробки інформації та прийняття рішень від даної підсистеми подається імпульс при розпізнаванні RFID-мітки, а далі основний контролер вмикає чи відключає режим «охорони».

ШДП1 – шлейф датчиків з вхідної групи, ШДП2 – спальня, ШДП3 – кухня-столова, ШДП4 – дитяча 2, ШДП5 – дитяча 1, ШДП6 – зовнішній периметр будинку, ШДП7 – периметр території ділянки.

В якості блоку обробки інформації та прийняття рішення використовуємо вільнопрограмований логічний контролер МахуСоп Flexy-S. Кількість дискретних входів у контролера МахуСоп Flexy-S є 14. Таким чином на шлейфи датчиків з приміщень задіяні 8 входів контролера. Таким чином задіяні 8 дискретних входів контролеру з 14 наявних.

В якості об'єктів управління (виконуючих механізмів) до виходів контролера підключаємо світлозвукову сирену та лампочку індикації стану сигналізації. Управління станом об'єктів управління носить дискретний характер – ця така дія на об'єкт, при якому він переходить, у відмінне від поточного, на свідомо певний стан. В нашому випадку це ввімкнення світлозвукової сирени та лампочки індикації стану системи.

2.3. Вибір обладнання для функціонування системи

Для забезпечення працездатності модулю сповіщувачів проведемо вибір обладнання. Враховуючи то факт, що господарі домоволодіння відмовились від встановлення відеокамер та на підставі проведеного аналізу базових рішень щодо охорони приміщень, пропонуємо використовувати для виявлення руху у середині будинку комбінований датчик руху та розриву скла SWAN PGB PGB, рис.2.5.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		31



Рисунок 2.5 – Датчик руху та розриву скла SWAN PGB PGB

Технічні характеристики:

- використовується для виявлення рухів людини і розбиття скла в приміщенні;
- счетверенний ІК-піроелектричний сенсором руху, акустичний сенсор розбиття;
- виявляє рух на відстані 18 метрів, горизонтальний кут огляду 105 °, розбиття скла на відстані 10 м, горизонтальний кут детектування 90 °;
- мікропроцесорна обробка амплітуди хвилі, ІК і мікрохвильового сенсора виключає помилкові спрацьовування;
- легко і швидко монтується на стіну;
- напівсферична лінза Френеля для оптимального огляду зони під датчиком;
- захищений від розтину тампер;
- імунітет від тварин вагою до 25 кг;
- підтримується будь-якими центральними, які працюють з НС шлейфами;
- присутній автоматична компенсація температурних перепадів;
- перемикач кількості імпульсів дозволяє вибрати режим роботи датчика для стабільної навколишнього середовища і для нестабільної (для виключення помилкових спрацьовувань);
- реалізовано режим тестування, в якому налаштовується чутливість датчика на розбиття скла, удари по склу, рух;
- світлодіодну індикацію при потребі можна відключити;

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

- чутливість звукового каналу крім ручного регулювання можна включити в режим 50% і 100%;
- захист від RF інтерференцій в частотному діапазоні 10 - 1000 МГц;
- захист від ЕМІ інтерференцій - 50 000 В;
- захист від спалахів світла (наприклад, від галогенною лампи на відстані 2,4 м);
- три світлодіода відповідають за сенсори і тривогу, зелений - індикатор удару, жовтий - розбиття скла, червоний – тривога.

Датчик руху і розбиття скла SWAN PGB призначений для відстеження руху людини в приміщенні, що охороняється і детектування ударів по склу та розбиття скла. Принцип дії зчотвереної сенсора руху заснований на визначенні інфрачервоного (ІЧ) випромінювання. Кожна жива істота - джерело ІК випромінювання. Як тільки датчик детектирует ІК-випромінювання в межах охоронної зони, він відсилає сигнал тривоги на центральний блок охоронної сигналізації. У датчику реалізований імунітет від тварин вагою до 25 кг і висотою до 1 м, спрацювання генерується тільки при русі людини. Якщо в приміщенні впаде який-небудь предмет, пробіжить кішка - датчик не спрацює. Вбудований електретний мікрофон дозволяє виявити удари по склу та розбиття скла. При цьому використовується захист від помилкових спрацювань. Вступник звук аналізується поетапно. Для включення тривоги спочатку повинні бути зроблені низькочастотні звуки (удар по склу), а потім - високочастотні (звук скла, що розбивається), тільки після цього відправиться сигнал тривоги. Комбінований датчик руху і розбиття скла використовується для охорони практично всіх об'єктів: заміських будинків, дач, офісів, торгових залів, квартир. Датчик руху - один з найпоширеніших елементів охоронних сигналізацій.

В якості герконового датчика використовуємо датчик магнітноконтактний (герконовий) СМК19, рис. 2.6.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		33



Рисунок 2.6 – Вигляд магнітоконтального датчика СМК19

Магнітоконтальный датчик відкриття геркон СМК19призначений для контролю відкриття дверей, вікон, воріт, люків і т. п. Тип контактів нормально розімкнуті, при піднесенні магніту контакти замикаються. Датчик виготовлений з якісного пластика білого кольору. Передбачений накладний тип монтажу, кріплення здійснюється за допомогою самоклеючої стрічки, для більш посиленого монтажу можна використовувати шурупи. Частина датчика з герконом рекомендується встановлювати на нерухому частину предмета а другу частину з магнітом на рухому. При установці датчика на металеві поверхні необхідно віддалити датчик від металу, для цього можна використовувати проставки (гумові, пластикові, дерев'яні). В датчику СМК19 використовується високоякісний геркон термін служби якого понад 1млн спрацьовувань. Датчик не вимагає подачі живлення і підтримується будь-якими центральними які працюють з НС (нормально замкнутими) шлейфами.

Технічні характеристики :

- тип датчика: магнітоконтальный;
- тип підключення: провідний;
- матеріал корпусу: пластик;
- метод установки: накладний;
- принцип роботи : на розмикання ланцюга;
- тип контакту: NO (нормально розімкнутий);
- робоча відстань:16 ~ 22 мм;
- діапазон робочих температур: -40...+50 °С;
- габарити, мм: 7 x 13 x 29;
- гарантія: 12мес;

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		34

- виробник: Україна.

Модуль безперебійного живлення призначених для забезпечення безперебійної роботи системи і розрахований на 24 години безперервної роботи в режимі навантаження.

В якості сигнальної сирени використовуємо внутрішню світлозвукову сирену Satel SP-500 R /BL/O, рис. 2.7.



Рисунок 2.7 – Провідна вулична світлозвукова сирена Satel SP-500 R /BL/O

Принцип роботи провідного вуличної світлозвукової сирени Satel SP-500 R/BL/O полягає в тому, що при отриманні сигналу з центрального блоку, включається сирена, сповіщаючи про тривогу не тільки звуком, а й світловим індикатором на корпусі. Звуковий сигнал генерується п'єзоелектричним перетворювачем, світлове оповіщення – яскравими світлодіодами. Акустична потужність сирени – 120 дБ.

Оснащена тамперної захистом від розтину корпусу і відривання пристрою від стіни. Встановлюється на плоску поверхню і призначена для зовнішнього монтажу (діапазон робочих температур -35 ° С до + 55 ° С). Живиться від приладу з напругою DC 12V і силою струму 400 мА. Акустична потужність - 120 дБ.

Для обробки інформації з блоку модулів сповіщення та прийняття управлінських рішень, використовуємо контролер Махусон Flexu-S рисунок 2.8.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35



Рисунок 2.8 – Контролер Махуcon Flexy-S

Технічні характеристики контролеру представлено в таблиці 2.1.

Таблиця 2.1

Технічні характеристики контролеру МахуConFlexy

Напруга живлення	~24 В, 50 Гц, =24 В	
Споживана потужність, не більше	10 Вт	
Програмування	«Конфігуратор FBD» і стандартну мову програмування FBD за стандартом IEC 61161-3	
Входи	аналогові – Pt1000 Ni1000,(0-10) В або дискретні з внутрішнім джерелом живлення	14 шт.
Виходи	аналогові -(0-10) В, 20 кОм	6 шт.
	дискретні беспотенціальні 6 А, ~250 В	10 шт.
Інтерфейси **	RS - 485, LON, ETHERNET	
Тип клавіатури	сенсорна	
	з інтерфейсним модулем	роз'єм
Спосіб зв'язку	з модулями розширення	провідний інтерфейс
Корпус	міра захисту 1P 20	
Підключення	дріт, перерізом не більше 1 мм ²	

В якості сигнальної лампочки про стан системи використовує сигнальну лампочку червоного кольору, рис. 2.9.



Рисунок 2.9 – Зовнішній вигляд сигнальної лампочки

Для організації захисту ззовні будинку, по периметру території ділянки домоволодіння розміщуємо активний інфрачервоний 4-променевий бар'єр LBW-100-4, рис. 2.10.



Рисунок 2.10 – Вигляді ІЧ-бар'єру LBW-100-4

Для перекриття всієї зони використовуємо 4 набори цього бар'єру. В такому разі створиться безперервна зона перекриття всієї ділянки. Призначений для виявлення порушника як в приміщенні, так і на вулиці. Бар'єр рекомендується використовувати для захисту дверей, вікон, воріт, складів з високими стелажми і для захисту периметрів. Бар'єр складається з двох частин: передавача (TRANSMITTER) і приймача (RECEIVER). У передавачі знаходяться діоди, випромінюючі інфрачервоні пучки світла, а в приймачі діоди, що приймають їх.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		37

Якщо хоч би два інфрачервоних променя перекриваються стороннім предметом або істотою, бар'єр переходить в режим "ТРИВОГА" і приймач передає сигнал на центральний блок охоронної сигналізації.

Технічні характеристики:

- тип датчика: дротовий;
- кількість інфрачервоних променів: 4;
- довжина ІЧ-променя: 100 м;
- горизонтальний кут налаштування променя: 180 градусів (± 90 градусів);
- вертикальний кут налаштування променя: нерегульований;
- швидкість відгуку: 40 msec;
- тампер: NC;
- виходи реле: NC/NO/COM (30V/1A);
- живлення: DC 11-18V;
- споживання: 90mA max;
- міра захисту: IP65;
- діапазон температур: - 25°C... 55°C;
- розміри: висота 76 см.

Для забезпечення моніторингу зовнішнього периметру будинку використовуємо датчик руху вуличний Crow EDS 2000, що призначений для відстеження руху людини на території, що охороняється, рис. 2.11.



Рисунок 2.11 – Зовнішній вигляд Crow EDS 2000

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		38

Пристрій володіє унікальною оптичною системою з пари незалежних один від одного піроелемент, що працюють в ІЧ-діапазоні , і СВЧ-приймача (ефект Доплера), з можливістю регулювання їх чутливості і дальності виявлення (до 6 значень в залежності від зовнішніх умов установки і експлуатації датчика). Такий функціонал мінімізує кількість помилкових спрацьовувань, наприклад, на рух птахів або невеликих тварин.

Принцип дії Crow EDS 2000 заснований на визначенні інфрачервоного (ІЧ) випромінювання. Кожна жива істота – джерело ІЧ випромінювання. Отже, як тільки датчик помічає його – відправляє сигнал тривоги на центральний блок охоронної сигналізації. Візуалізація роботи здійснюється за допомогою світлодіодного підсвічування.

Сповіщувач виконаний в герметичному полікарбонатному корпусі з захистом від пошкоджень, сонячного світла, вітру (до 30 м/с). Передбачає настінний вуличний монтаж на висоті до 1,8-2,4 м. В комплекті йде спеціальна маска на фокусуються лінзу, що дозволяє контролювати спрацювання датчика на тварин (датчик ігнорує тварин масою до 15 кг без маски і до 35 кг з встановленою маскою).

Функції та особливості:

- призначений для виявлення рухів людини на території, що охороняється;
- можливістю регулювання чутливості і дальності виявлення (до 6 значень в залежності від зовнішніх умов установки і експлуатації датчика);
- імунітет від домашніх тварин: до 35 кг;
- діяльність визначення руху: до 15 м;
- мікропроцесорна обробка сигналу;
- подвійний чотирьох променевий піроелемент, рис. 2.12;
- автоматична термокомпенсація;
- діаграма спрямованості: 90 °;
- тривожні виходи: АЛЕ, НЗ - 28V, 0,1А з навантаженням 10 Ом;
- спеціальна маска на фокусуються лінзу в комплекті;

- полікарбонатний корпус із захистом від пошкоджень, сонячного світла, вітру;
- тамперний захист від несанкціонованого доступу.

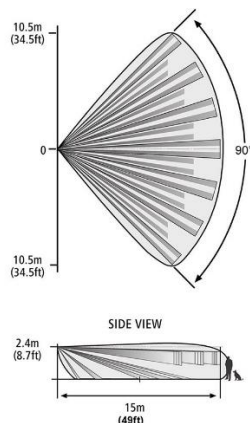


Рисунок 2.12 – Діаграма направленості датчика руху Crow EDS 2000

RFID-технології використовуємо для постановки та зняття об'єкту з режиму «охорона». В якості зчитувача використовуємо Автономний контролер з вбудованим RFID зчитувачем стандарту EM-Marin 125KHz.



Рисунок 2.13 – Автономний контролер з вбудованим RFID зчитувачем

Розрахований на роботу до 2000 карт / ключів. Робоча частота 125 кГц. Дальність зчитування 0-10см. Вихід реле NC, NO, COM. Звукова / світлова індикація. Імпульсний і тригерний режими роботи. Споживання 80 мА. Струм комутації 1А. Живлення 12В. Захист IP68, водонепроникний. Корпус зроблений з металу сірого кольору. Розміри 85x85x15мм.

Для забезпечення належного функціонування системи охорони периметру домоволодіння використано наступний перелік елементів:

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		40

Перелік елементів системи охорони

Назва засобу	Кількість, од.
Датчик руху та розриву скла SWAN PGB PGB (внутрішній)	5
Датчик магнітноконтактний (герконовий) СМК19	6
Провідна вулична світлозвукова сирена Satel SP-500 R /BL/O	1
Контролер МахуConFlexy-S	1
Сигнальна лампочка, червона	1
Активний інфрачервоний 4-променевий бар'єр LBW-100-4	4
Датчик руху вуличний Crow EDS 2000	4
Автономний контролер з вбудованим RFID зчитувачем	1

Схема розміщення активного інфрачервоного 4-променевого бар'єру LBW-100-4 та датчиків руху вуличних Crow EDS 2000 представлено на рисунку 2.14.

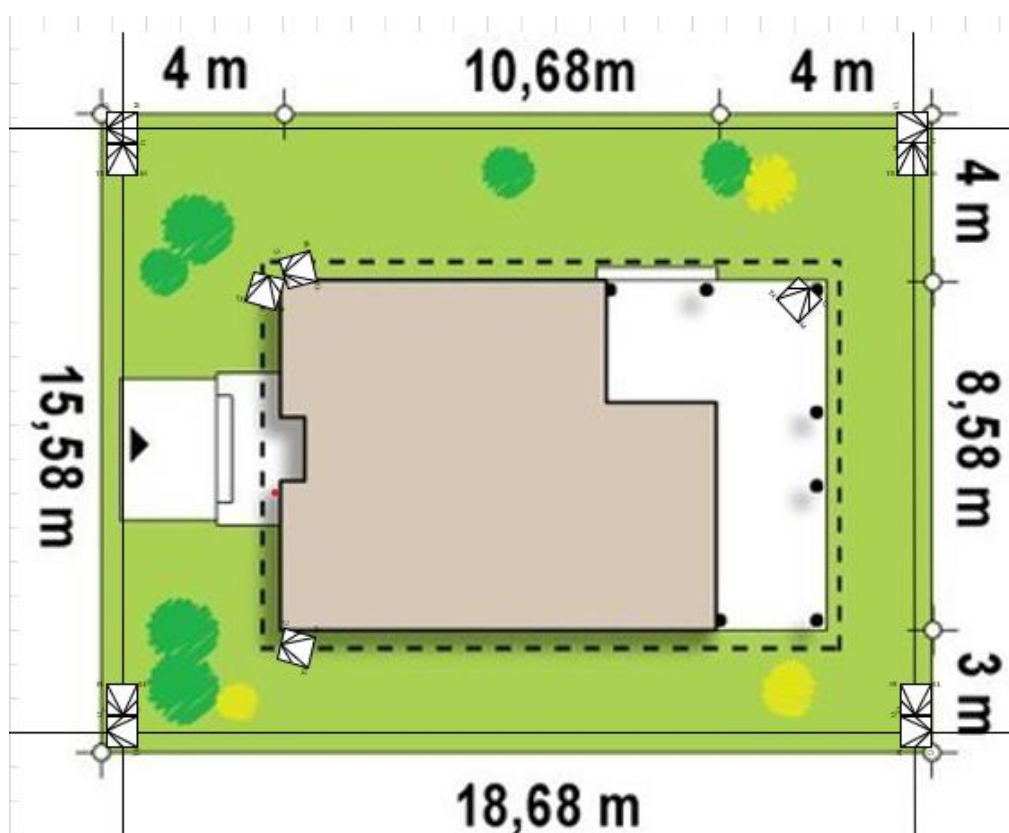


Рисунок 2.14 – Схема розміщення засобів охорони ззовні будинку

Як видно з рисунку, 2.14 по зовнішньому периметру будинку розміщено 4 вуличні датчики руху, зокрема 1 на терасі, інші забезпечують виявлення руху по іншим трьом сторонам будинку. По периметру ділянки домоволодіння розміщено 4 набори ІЧ-бар'єру. Кожен набір (передавач-приймач) забезпечують виявлення по стороні ділянки, рис. 2.15.

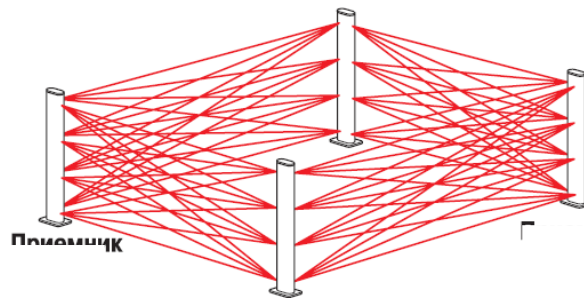


Рисунок 2.15 – Схема ІЧ променів по периметру ділянки

Схема розміщення засобів охорони представлена на рис.2.16

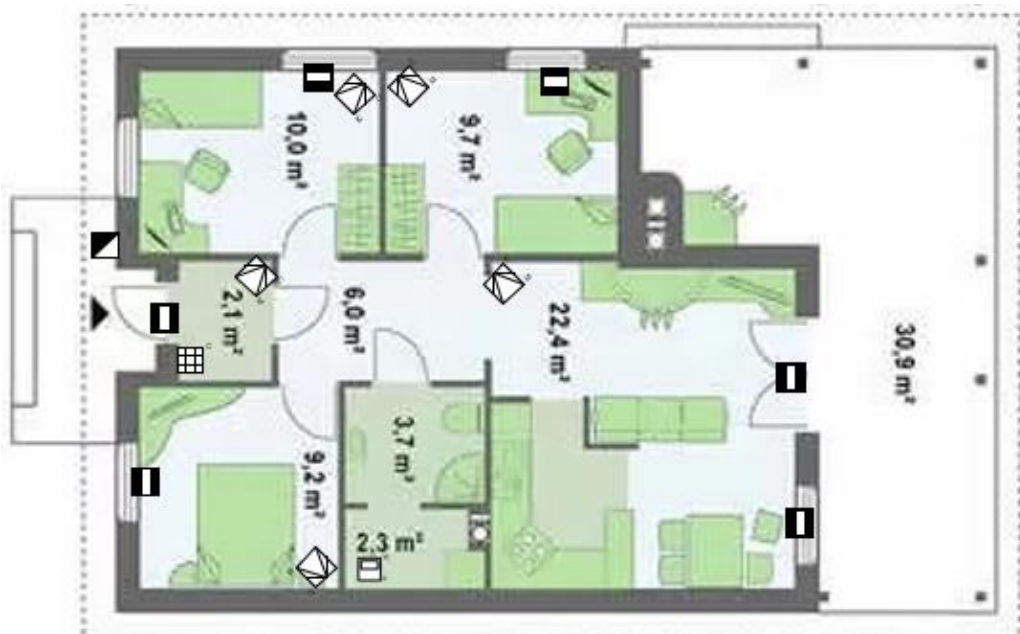


Рисунок 2.16 – Схема розміщення датчиків всередині будинку

На даній схемі використовуються наступні умовні позначення:



– сповіщувач магнітно-контактний (герконовий);



– сповіщувач оптико-електронний пасивний (датчик руху);



– контролер;

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		42

■ – світлозвукова сирена;



– панель RFID.

Основні елементи для функціонування системи охорони периметру домоволодіння вибрано, подальші дослідження будуть направлені на монтажні роботи та програмування контролера.

З урахуванням вибраного обладнання проводимо розробку схеми електричної принципової щита керування системою, де показується підключення шлейфів датчиків та виконавчих механізмів до блоку управління, рис.2.17.

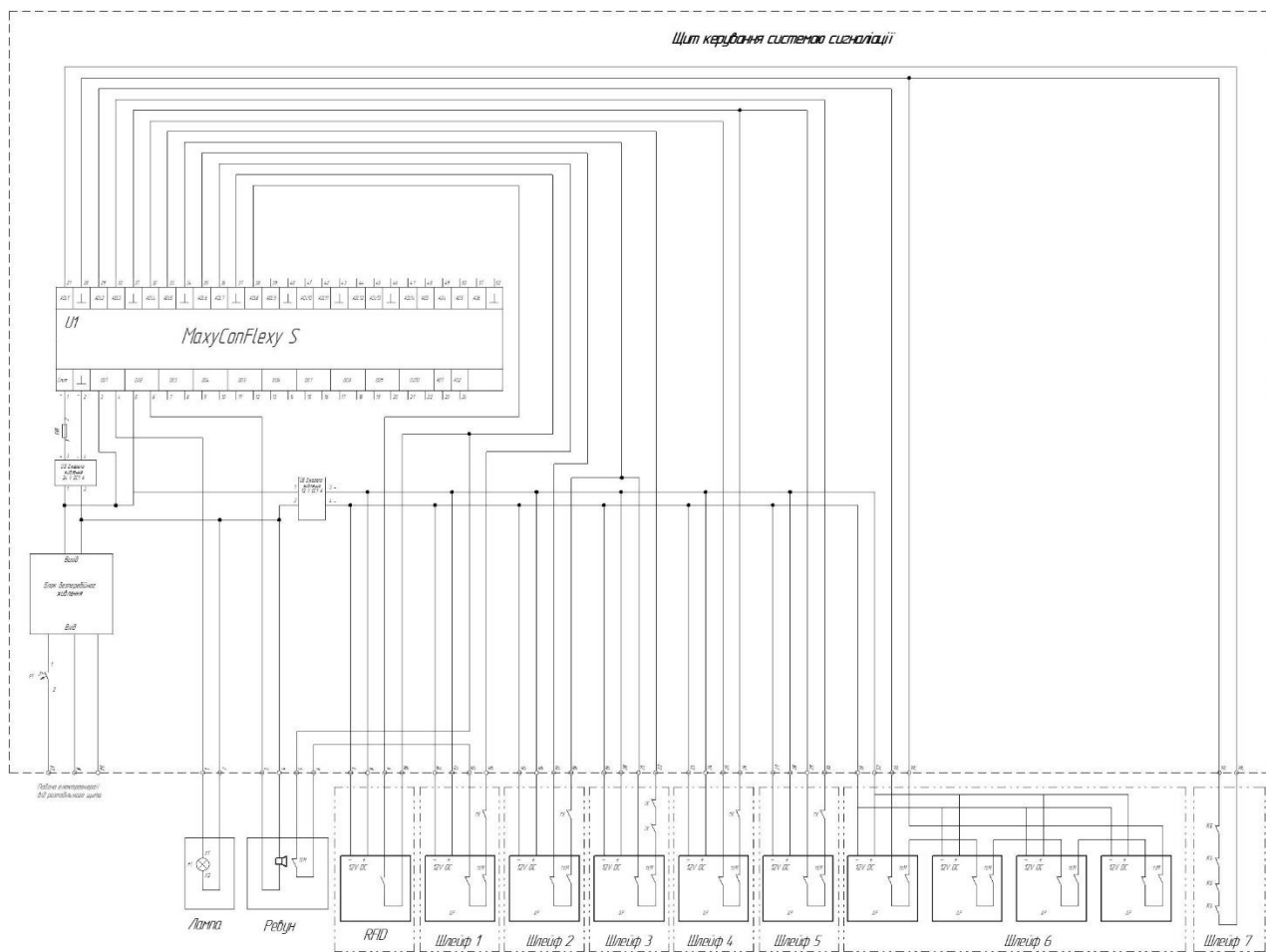


Рисунок 2.17 – Схема електрична принципова щита керування системою

Монтаж контролеру та комутаційних пристроїв виконуємо в шафі з використанням монтажної рейки. При монтажі системи на DIN-рейку варто, також, використовувати кінцеві зажими з кожного кінця рейки. Застосування

кінцевих зажимів затримує системний блок при горизонтальних переміщеннях уздовж рейки. Це дозволяє мінімізувати можливості випадкового натягу чи обриву ліній зв'язку. На задній панелі системного блоку розміщені два невеликі утримуючі зажими. При монтажі системного блоку на DIN-рейку варто установити блок на рейку й обережно підняти утримуючі зажими, що замикають систему на рейці. Для зняття системного блоку, у свою чергу, необхідно опустити зажим, відвести вгору на себе нижню частину блоку, а потім зняти його з рейки. Для комутації датчиків використовувався кабель ПВС 2х0,75 мм². Для заливки програми на контролер використовується SD-карта пам'яті.

Система використовується в якості єдиного локального пристрою контролю і управління.

Висновки до розділу 2

1. Проведено аналіз розміщення домоволодіння та самого будинку.

2. Проведений аналіз об'єкту дослідження дозволив сформувати структурну схему функціональних модулів системи охорони периметру домоволодіння, яка включає модуль сповіщувачів, модуль виконавчих механізмів, модуль безперебійного живлення, підсистему управління доступу та охорони об'єкту.

3. Розроблено функціональну схему системи охорони периметру домоволодіння, яка складається з вхідного блоку, блоку обробки інформації та прийняття рішень, а також блоку виконавчих механізмів. Блок обробки інформації та прийняття рішень підключено до мережі Інтернет, що дає можливість відправляти всі дані з контролеру на веб-сервер.

4. Проведено вибір обладнання для функціонування системи та розроблено схеми розміщення засобів охорони по периметру території та всередині будинку.

5. Розроблено схему електричну принципової щита керування системою охорони периметру домоволодіння.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		44

3. РОЗРОБКА БЛОК-СХЕМИ АЛГОРИТМУ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ

3.1. Розробка блок-схеми алгоритму

Згідно з вище визначених вимог, можна чітко сформулювати задачі, які має виконувати запропонована система. Проаналізувавши методи реалізації заданого функціоналу програми, можемо побудувати алгоритм за яким спроектована система охорони периметру домоволодіння буде працювати.

Реалізована схема загальної блок-схеми алгоритму роботи програми зображена на рисунку 3.1. Початок програми включає в себе безпосередньо запуск програмного додатку шляхом занесення у контролер. Після початку роботи програмного продукту для можливості відслідковування порушень периметру необхідно ввімкнути сигналізацію. Для цього потрібно запустити систему, тим самим подаючи імпульсний сигнал на контролер (1). Якщо ж нічого не вводити, то сигналізація приміщення не буде ввімкнена (11) і буде заходитись у стані очікування сигналу включення.

Якщо сигналізація ввімкнена (2), то система переходить у режим охорони, то при на екрані контролера з'являється надпис про включення та вмикається індикаційна лампочка (3). Після цього починається активна фаза роботи контролера – відбувається зчитування інформації зі шлейфів датчиків. Так при спрацюванні сигналізація (5): спрацьовує світлозвукова сирена (6), та на головне вікно виводиться назва приміщення, де виявлено порушення периметру (7) та передається сигнал тривоги власнику через Веб-сервер. Такий стан система утримує доки не зніметься стан тривоги (9). Коли власник знімає стан тривоги, то пропадає надпис з екрану монітору та система переходить у режим вимкнення та очікування на включення (10). Далі робота контролера повторюється, він знову починає відслідковувати дії, що відбуваються та виводити цю інформацію на екран.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						45
Змн.	Арк.	№ докум.	Підпис	Дата		

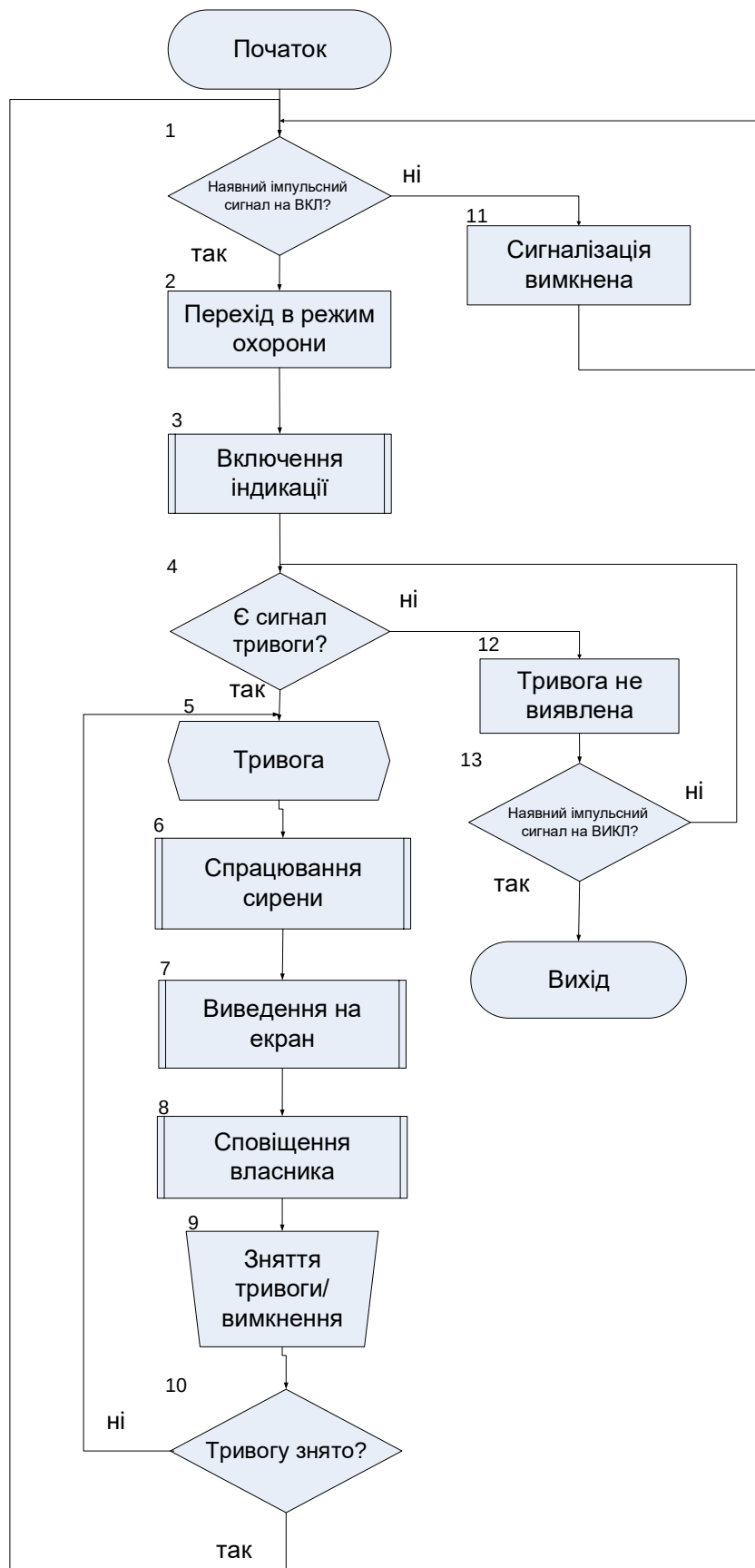


Рисунок 3.1 – Блок-схема алгоритму

Тепер розглянемо іншу гілку роботи системи. Якщо система протягом своєї роботи не виявила порушень периметру (12), система знаходиться в режимі

Змн.	Арк.	№ докум.	Підпис	Дата

КБ.КР.Б – 125 – 08 – ПЗ

Арк.

46

очікування імпульсного сигналу, якщо сигнал надійшов (13), то система завершує свою роботи, якщо ні, знаходиться в режимі охорони периметру (4).

Якщо ж було зафіксовано спрацювання сигналізації, то потрібно усунути визначену проблему для відновлення нормальної роботи контролера. Для цього було розроблено алгоритм відновлення роботи системи, який представлено на рисунку 3.2.

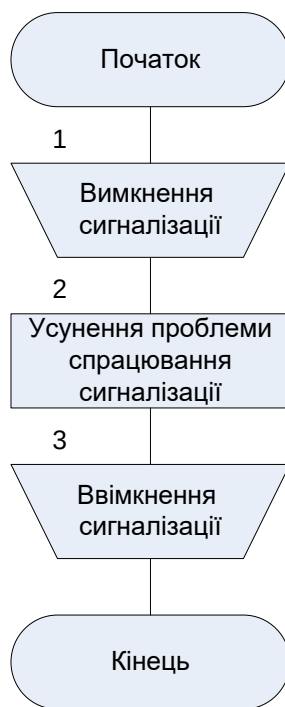


Рисунок 3.2 – Схема алгоритму відновлення роботи системи

Отож, для відновлення нормальної роботи контролера необхідно: вимкнути сигналізацію (1); провести перевірку хибності спрацьовування сигналізації (2) у разі необхідності затримати порушника та знову ввімкнути сигналізацію.

3.2. Розробка програми для роботи контролера

Програмування контролера МахуСоп Flexy на вирішення задач управління системою сповіщувачів несанкціонованого доступу в приміщення відбувається за допомогою спеціального програмного середовища в емуляторі роботи контролера «Конфігуратор FBD».

Для встановлення конфігураційних характеристик входів контролера необхідно вибрати вхід та натиснути праву кнопку миші. Після цього відкриється діалогове вікно, що представлене на рисунку 3.3 – «Свойства блока ADI_0.1»

Обираємо тип датчика «Дискретный» із випадаючого списку, та додаємо коментар для кращого розпізнавання пристроїв

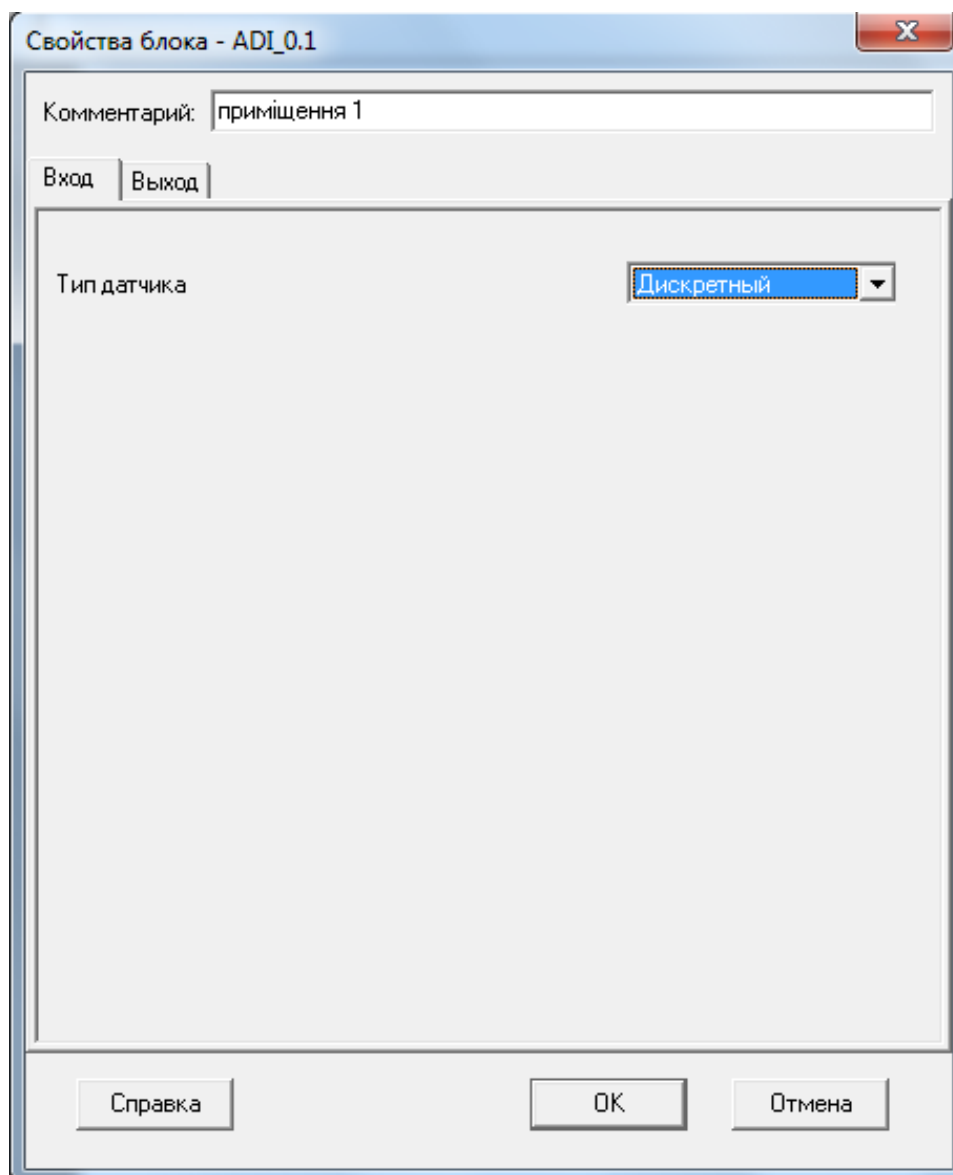


Рисунок 3.3 – «Свойства блока ADI_0.1»

Дана операція проводиться для всіх задіяних входів (у нашому випадку 8 входів), в результаті чого отримуємо вигляд, рисунок 3.4.



Рисунок 3.4 – Налаштування входів контролеру

На наступному етапі необхідно провести налаштування конфігураційних параметрів виходу. Для цього необхідно вибрати потрібний вихід та провести налаштування, рисунок 3.5.

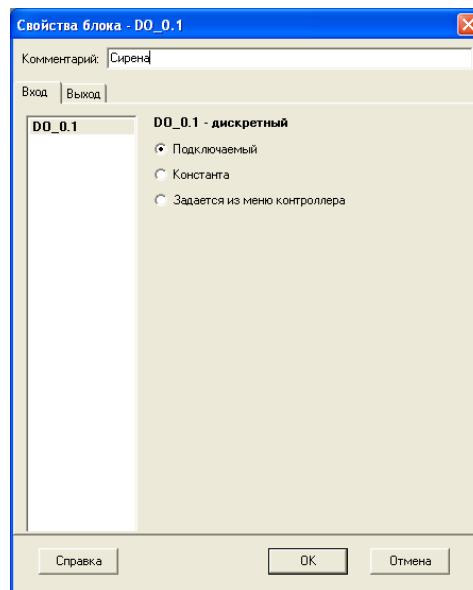


Рисунок 3.5 – Вигляд вікна для налаштування виходів контролеру

Враховуючи той факт, що на виході контролеру підключено світлозвукову сирену та індикаційну лампочку, то ми задіємо тільки два виходи. Провівши налаштування виходів отримуємо наступний вигляд виходів, рисунок 3.6.



Рисунок 3.6 – Задіяні виходи контролеру

Враховуючи особливості датчиків, що використовуються, нам необхідно для коректності роботи програми управління провести інверсію входів. Для цього використовуємо логічний елемент «НЕ». Оскільки задіяно 7 входів на шлейфи приміщень, то відповідно використовуємо 7 логічних елементів «НЕ», рисунок 3.7.

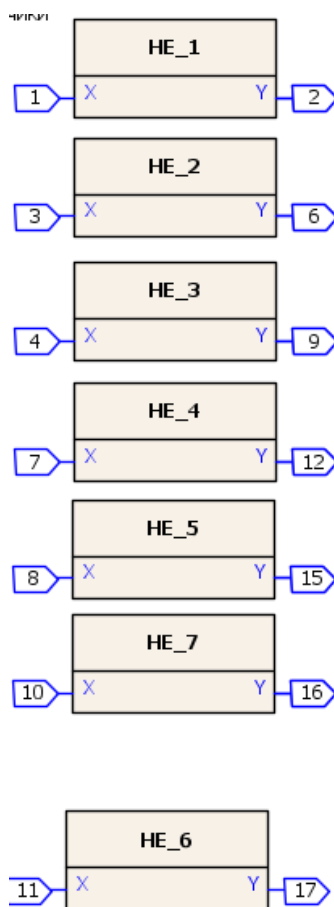


Рисунок 3.7 – Інверсія входних сигналів

Наступним елементом нашої програми управління є «RS тригери». «RS тригер_1»– «RS тригер_7» використовуються для виведення на екран сигналу тривоги та фіксації значення до відключення сигналізації, рисунок 3.8.



Рисунок 3.8 – Затримка сигналу тривоги по приміщенням

Алгоблок «Ключ 2-х поз. Дискр_3», рисунок 3.9 передає один із сигналів який знаходиться на входах X1 (спрацювання одного із шлейфів, 0 – норма, 1–

тривога) та X2 (відсутність сигналу, 0) на вихід Y в залежності від того, що будемо подавати на вхід Q. Якщо Q=0 (сигналізація вимкнена) то на виході буде значення X2 тобто 0, а якщо Q=1 (сигналізація ввімкнена) то буде подаватися значення з X1. Тригер «RS тригер_13» застосовується для фіксації значення «тривога» до відключення сигналізації, тобто подача сигналу «1» на вхід «Reset» тригера «RS тригер_13» та подача сигналу на вихід, тобто включення звукової та світлової індикації «тривога».

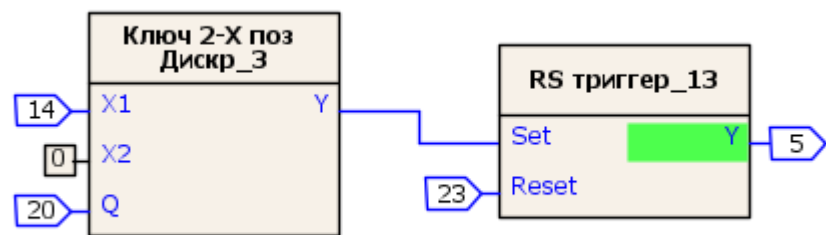


Рисунок 3.9 – Набір блоків для фіксації значення «тривога»

Блок «ИЛИ_2» призначений для виявлення сигналу тривоги по шлейфам приміщень. Таким чином при появі «1» на будь-якому з входів (X1–X11) на виході ми отримуємо «1», рисунок 3.10, яка подається на попередньо описаний елемент («Ключ 2-Х поз. Дискр_3»)

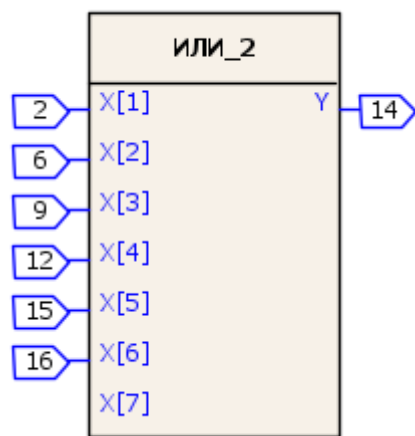


Рисунок 3.10 – Блок виявлення сигналів тривоги по шлейфам

Для включення та виключення сигналізації за допомогою меню контролера або RFID-мітки використовуємо ряд блоків, що представлені на рисунку 3.11.

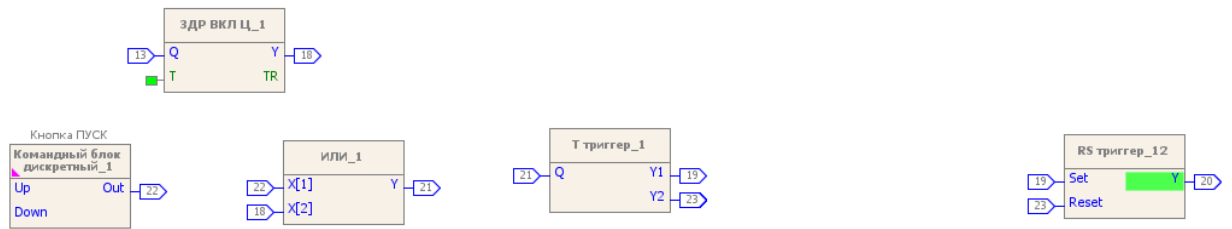


Рисунок 3.11 – Блоки для реалізації включення системи

В результаті проведених операцій та визначення блоків програми управління отримано наступний вигляд «Головної діаграми», рисунок 3.12.

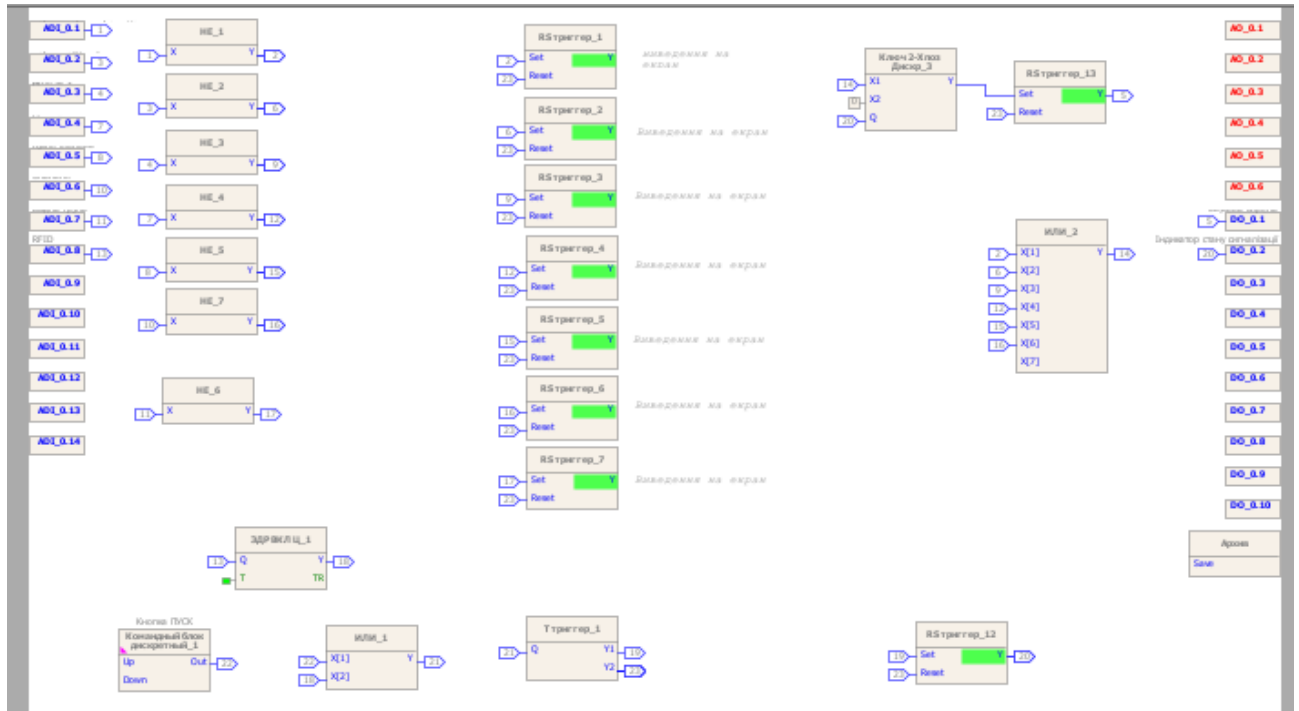


Рисунок 3.12 – Головна діаграма програми роботи контролера

Вигляд меню контролера представлено на рис. 3.13.

ТРИВОГА ЗОВН.ПЕРИМ ВНУТР.ПЕРИМ ДИТЯЧА 1 ДИТЯЧА 2 ВХІДНА ГРУПА КУХНЯ-СТОЛОВА СПАЛЬНЯ	 Сигналізація Ввімкнена
Час увімкнення сигналізації	0

Рисунок 3.13 – Вікно меню контролера

Як видно з рисунку 3.13, представлено тривоги по всіх шлейфам приміщень. У разі спрацювання будь-якого засобу захисту, на екрані контролера, а також визначеному гаджеті власника буде відображатися слово «ТРИВОГА» та нижче показано в якому саме приміщенні будинку, або по його периметру стався інцидент. Також відображається стан системи – «Ввімкнена» або «Вимкнена». Піктограма  служить для ввімкнення-вимкнення системи. Знизу відображається час роботи системи з моменту включення.

3.3. Тестування системи

Проводимо запуск розробленої програми на тестування. Для цього в меню програми RAUT Qubix натискаємо піктограму , що призводить до компіляції програми та її запуску в режимі симуляції роботи, рис. 3.14.

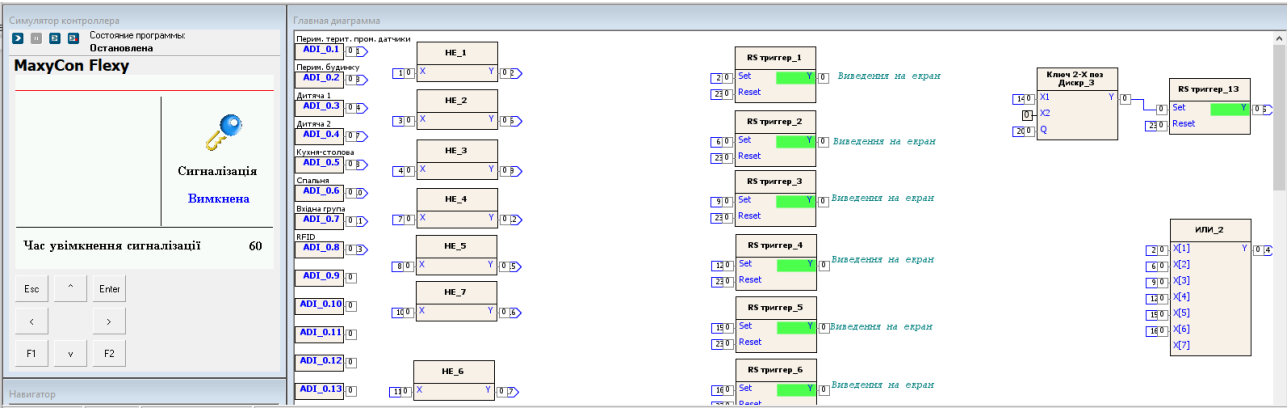


Рисунок 3.14 – Вигляд екрану при запуску симуляції

Як видно з рисунку, у лівій частині вікна відображається екран контролера, а праворуч стан елементів контролера. Натиснувши , ми побачимо загальний вигляд системи, рис. 3.15, де у правому вікні зліва знаходяться виходи датчиків, посередині сам контролер і праворуч входи виконавчих механізмів. Запуск програми здійснюється натиском на піктограму . Далі починається відлік роботи системи, рис. 3.16.

Імітацію спрацювання датчиків проводимо в ручному режимі. Для цього ми можемо вибрати будь-який задіяний вхід та відповідно натиснути на ньому два

рази лівою клавішою миші. Після цього з’явиться вікно значень параметрів даного входу, рис. 3.17.

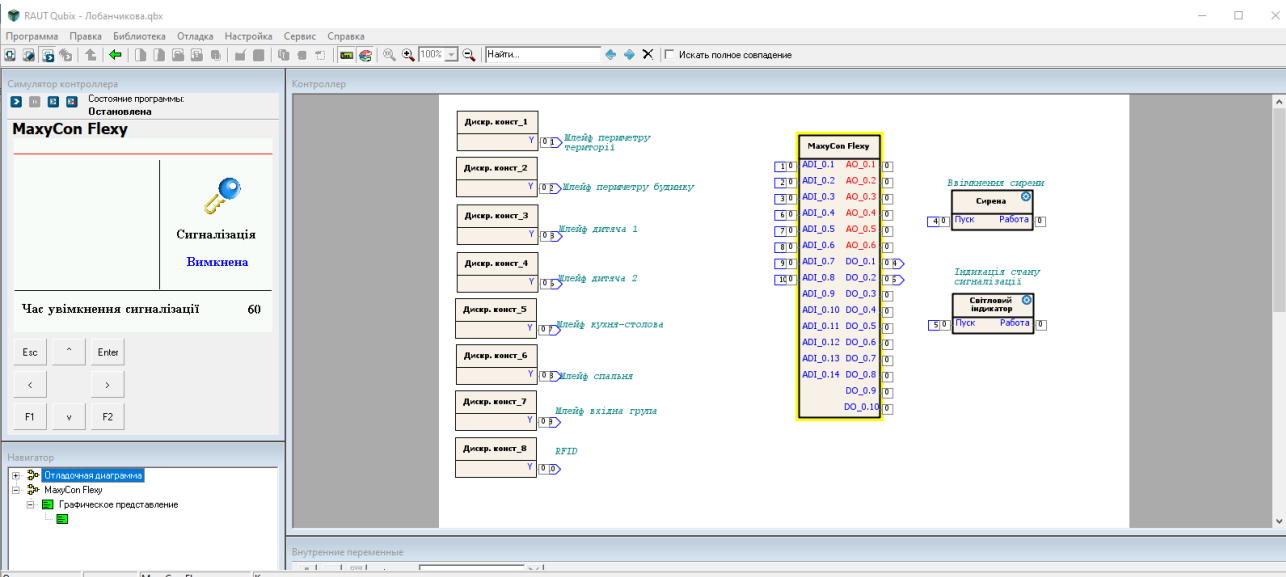


Рисунок 3.15 – Вікно відображення стану елементів системи та меню контролера в режимі симуляції

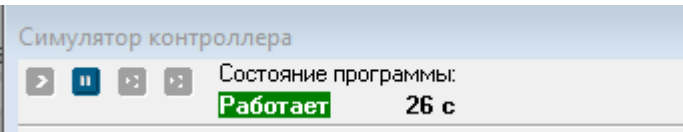


Рисунок 3.16 – Вікно відображення стану програми

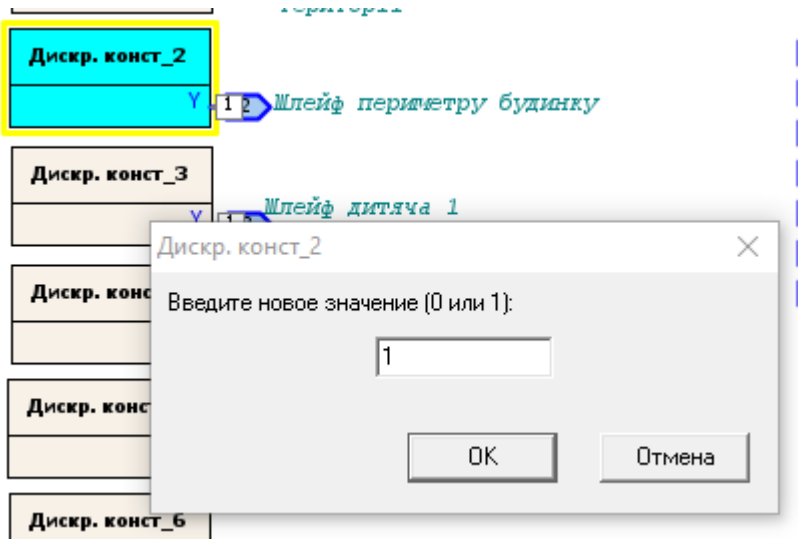


Рисунок 3.17 – Вікно задавання значень входу

У вікні, рис. 3.17 проводимо зміну значення «1» на «0», рис. 3.18 і спостерігаємо за реакцією системи, рис. 3.19.

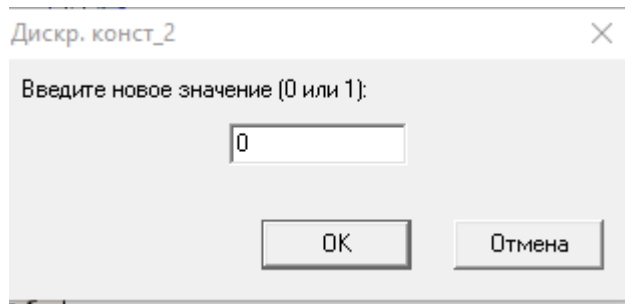


Рисунок 3.18 – Зміна значення параметру дискретного входу 2

На дискретний вхід 2 подається стан датчиків шлейфу периметру будинку, тобто датчиків руху, що розміщені ззовні будинку.

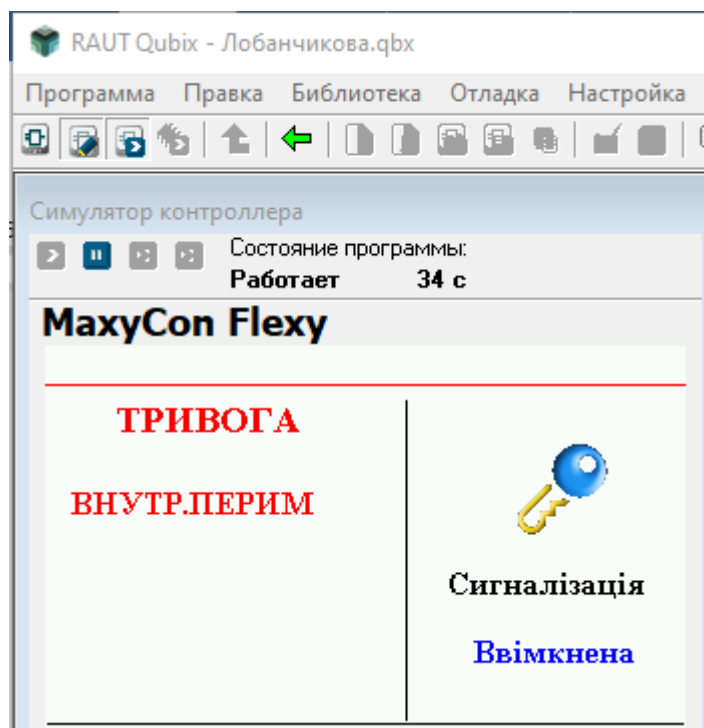


Рисунок 3.19 – Меню екрану контролера після введенного значення

Як видно з рисунку 3.19, система миттєво спрацювала і на екрані контролеру ми бачимо повідомлення про тривогу та зону в якій це відбулося. Зміну параметрів входу та виходу задіяних відповідних елементів можна побачити на рис. 3.20. Порівнявши рис. 3.15 та 3.20 бачимо, що система правильно зреагувала на імітацію спрацювання датчика та вивела повідомлення на екран, включила світлозвукову сирену.

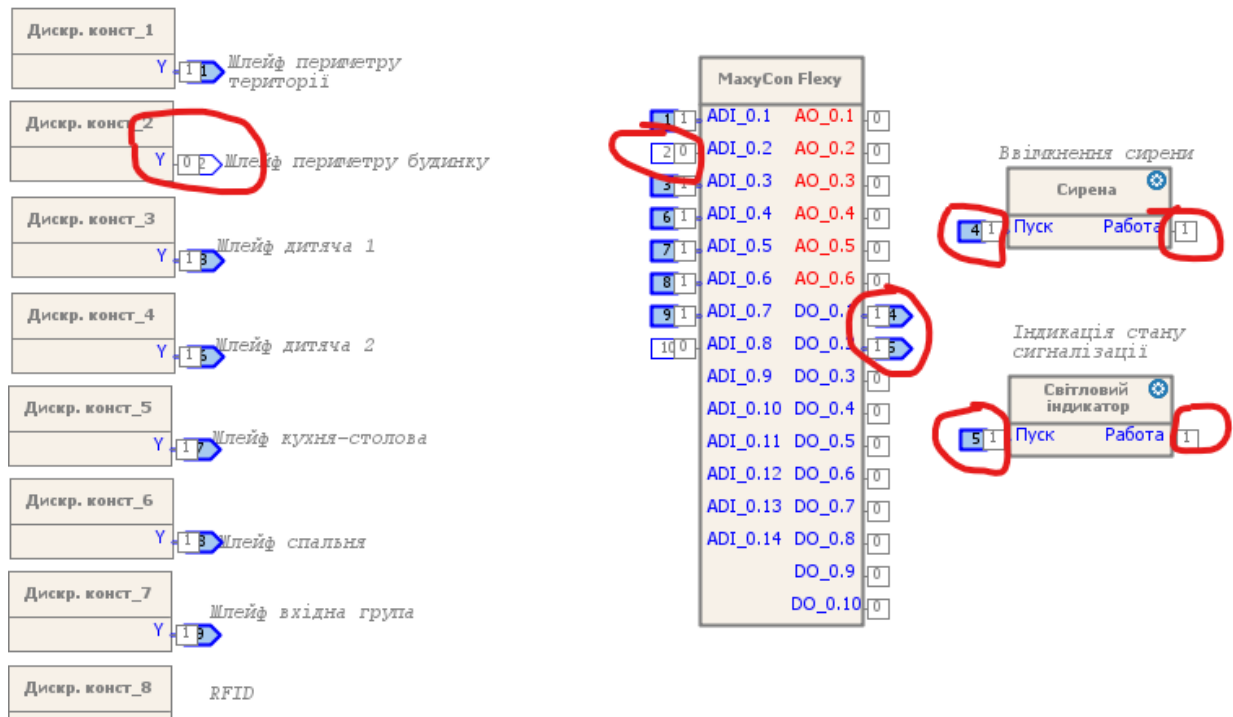


Рисунок 3.20 – Стан системи після зміни параметрів датчика 2

Таким чином здійснено перевірку і інших шлейфів, в результаті яких доведено, що програма працездатна, а система правильно реагує на зміну значень датчиків.

3.4. Аналіз кіберзагроз компонентів системи при реалізації на базі IoT

Системи охорони периметру території є складними інтегрованими комплексами. Поєднання різних технологій та засобів різних виробників збільшує ймовірність виникнення кіберзагроз та зростання вразливостей системи. При проектуванні системи охорони периметру домоволодіння нами використано провідні технології для реалізації системи, однак дана реалізація здійснюється, як правило при проектуванні будинку, або на стадії ремонту, так як встановлення такої системи вимагає прокладання кабелів (проводів) у штробу, що дозволяє зробити маскування системи для уникнення прямого електромагнітного впливу та безперешкодного підключення до системи з метою виведення її з ладу в цілому або її компонентів. Останнім часом все більшого попиту набувають безпроводні системи охорони периметру, в тому числі IoT

системи.

В межах даного дослідження проведемо аналіз кіберзагроз систем охорони периметру на прикладі IoT системи охорони периметру об'єкту, що функціонує на бездротових мережах передачі даних. В структуру входить множина датчиків руху **H**, RFID-зчитувачів RFID-міток **F**, герконових датчиків **GR**, шлюз та безпосередньо IoT монітор у вигляді СППР системи.

Входження людства в четверту промислову революцію (INDUSTRY 4.0) [19] 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.

Найбільша кількість атак припадає на портативні пристрої, використання безпроводних технологій зв'язку між елементами системи створює передумови для здійснення кібератаки на систему. Відповідно до [19] 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. [19], свідчить про таке:

- уразливості («дірки») в сучасних системах захисту уможлиблюють до 65 % кіберінцидентів;
- людський фактор – критичне (якщо масштабувати його до кількості та ступеня складності кіберзагроз) зниження рівня грамотності користувачів – до

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		58

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 ІТ-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 [19].

Досліджувальна нами система є бездротовою IoT системою, апаратна частина якої може бути розділена на наступні елементи, рис. 3.21 [19-28]:

- 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.

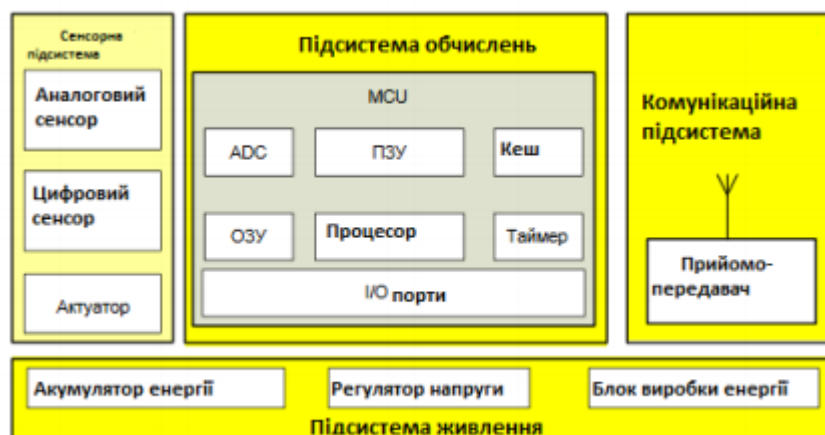


Рисунок 3.21 – Апаратна частина вузла IoT системи

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 природного середовища.

Враховуючи той факт, що сенсорні мережі вразливі до безлічі атак, особливо актуально питання забезпечення кіберзахисту ставиться при впровадженні 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 [19-28], рис. 3.22:

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

фізичного рівня:

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

канального рівня:

- атака зіткнень;

✓ атаки на протоколи маршрутизації:

- атака «Чорна діра»;
- селективна експедиторська атака;
- атака «Стрімкий натиск»;
- атака «Воронка»;

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						60
Змн.	Арк.	№ докум.	Підпис	Дата		

- атака «Сібіл»;
- атака «червоточини»;
- флуд атака;

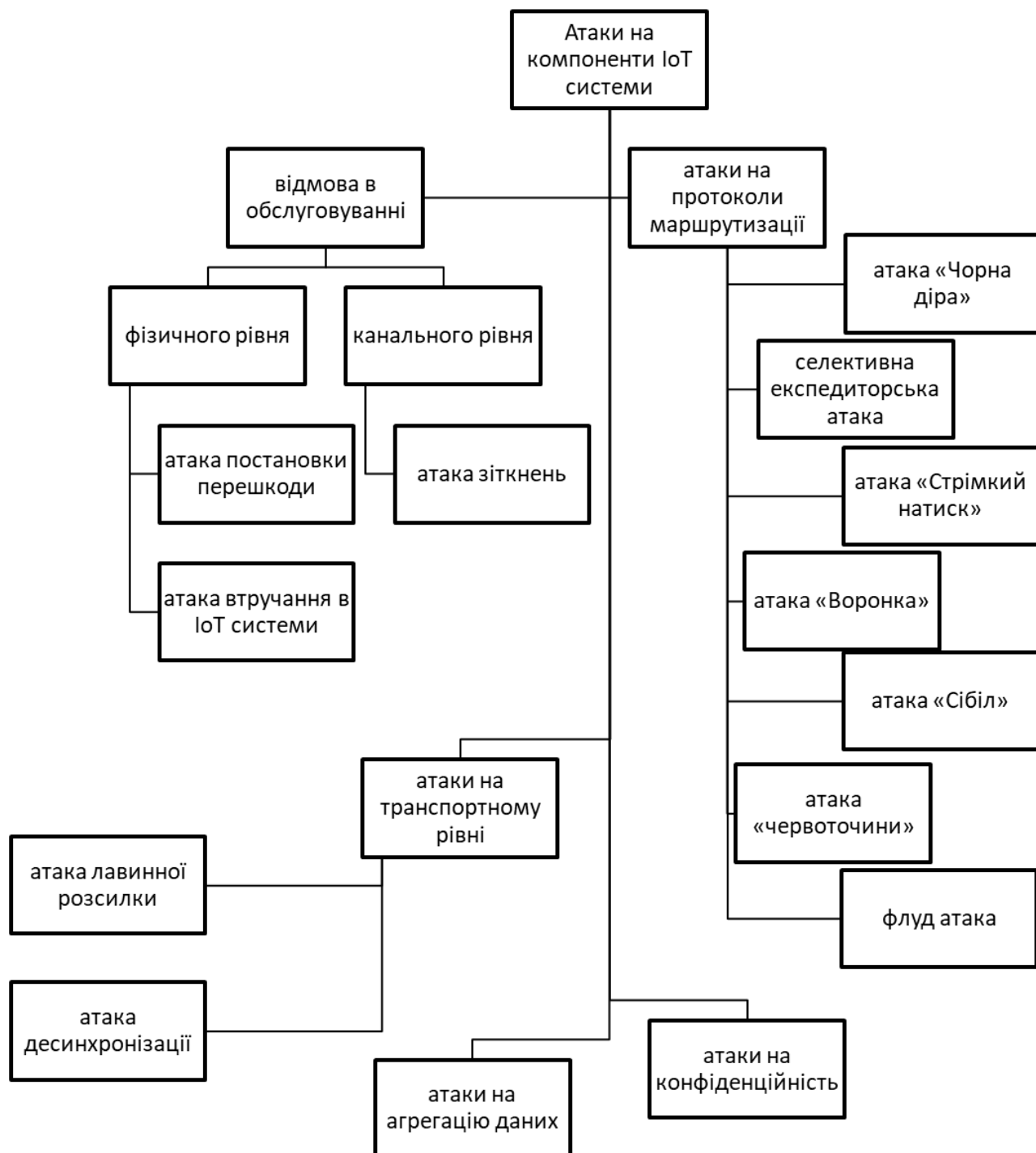


Рисунок 3.22 – Атаки на компоненти IoT системи

✓ 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 каналного рівня. DoS атака зіткнень на каналному 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 зломисник, 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 зломисник 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, зломисник прослуховуючи канал, повідомляє сусідів про те, що «знає» найкоротший маршрут до базової станції. Як тільки йому вдалося стати між транслуючим сенсорним вузлом і базовою станцією, він може виконувати будь-які дії з пакетам даних, що надходять до нього.

Атака «Сібіл» характеризується тим, що зломисник 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

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		63

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, каналної 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 посилку 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

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						64
Змн.	Арк.	№ докум.	Підпис	Дата		

(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 зломисник 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 зломисником 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.

Рекомендації щодо протидії вищезазначеним атакам можна викласти наступним чином. 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

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		65

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 спрацюванні 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 злоумисник до нього наблизиться впритул.

Для протидії DoS-атака каналного 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

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						66
Змн.	Арк.	№ докум.	Підпис	Дата		

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 каналному 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.

Висновки до розділу 3

1. Проведено розробку блок-схеми алгоритму роботи системи охорони периметру домоволодіння.

2. Проведена розробка та тестування програми функціонування системи охорони периметру домоволодіння, суттю якої є управління системою охорони приміщень від несанкціонованого доступу на базі контролера MaхуConFlexу за допомогою спеціального програмного середовища в емуляторі роботи контролера «Конфігуратор FBD».

3. Засобами комп'ютерного моделювання проведено симуляцію роботи спроектованої системи в результаті якого перевірено функціональність та правильність роботи програми для роботи контролера MaхуConFlexу, що написана на графічній мові програмування FBD (Function Block Diagram), яка стандартизована міжнародним стандартом IEC 61131-3.

4. Проведено аналіз та узагальнення кіберзагроз на компоненти IoT систем результаті якого визначено, що найбільша кількість атак припадає на вузли мережі, а використання безпроводних технологій зв'язку між елементами системи створює передумови для здійснення кібератаки на систему. В результаті проведеного аналізу і узагальнення розроблено рекомендації з протидії атакам на компоненти IoT системи.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						68
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

1. В результаті проведеного аналізу систем охорони периметру визначено, що є три класи систем, а саме дротові, бездротові та GSM-сигналізації. Комплектація систем, що представлені на ринку є типовими. Всі сигналізації масштабується за допомогою додаткових сенсорів.

2. Проведено аналіз та узагальнення кіберзагроз на компоненти IoT систем результаті якого визначено, що найбільша кількість атак припадає на вузли мережі, а використання безпроводних технологій зв'язку між елементами системи створює передумови для здійснення кібератаки на систему. Таким чином провідні системи мають більшу стійкість до зламу.

3. Проведений аналіз розміщення домоволодіння та самого будинку дозволив сформулювати структурну схему функціональних модулів системи охорони периметру, яка включає модуль сповіщувачів, модуль виконавчих механізмів, модуль безперебійного живлення, підсистему управління доступу та охорони об'єкту.

4. Розроблено функціональну схему системи охорони периметру домоволодіння, яка складається з вхідного блоку, блоку обробки інформації та прийняття рішень, а також блоку виконавчих механізмів. Блок обробки інформації та прийняття рішень підключено до мережі Інтернет, що дає можливість відправляти всі дані з контролера на веб-сервер.

5. Проведено вибір обладнання для функціонування системи та розроблено схеми розміщення засобів охорони по периметру території та всередині будинку. Розроблено схему електричну принципової щита керування системою охорони периметру домоволодіння

6. Проведено розробку блок-схеми алгоритму роботи системи охорони периметру домоволодіння. Проведена розробка та тестування програми функціонування системи охорони периметру домоволодіння, суттю якої є управління системою охорони приміщень від несанкціонованого доступу на базі контролера МахуConFlexu за допомогою спеціального програмного середовища

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		69

в емуляторі роботи контролера «Конфігуратор FBD».

7. Засобами комп'ютерного моделювання проведено симуляцію роботи спроектованої системи в результаті якого перевірено функціональність та правильність роботи програми для роботи контролера МахуConFlexy, що написана на графічній мові програмування FBD (Function Block Diagram), яка стандартизована міжнародним стандартом ІЕС 61131-3.

8. В результаті проведеного аналізу і узагальнення розроблено рекомендації з протидії атакам на компоненти безпроводних систем.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						70
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Охорона периметру / Гіпермаркет Безпеки «BEZPEKA SHOP». Режим доступу: https://www.bezpeka-shop.com/ua/catalog/okhrana_perimetra/.
2. 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.
3. 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
4. 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.
5. 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.
6. Корченко А.Г. Построение систем защиты информации на нечетких множествах [Текст] : Теория и практические решения / А.Г. Корченко. – К. : МК-Пресс, 2006. – 320 с
7. Грайворонський М.В. Безпека інформаційно-комунікаційних систем [Текст] / М.В. Грайворонський, О.М. Новіков – К.:Видавнича група bhv, 2009.– 608 с.
8. 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.
9. Кавун, С. В. Інформаційна безпека: підручник / С. В. Кавун. – Харків: Вид. ХНЕУ, 2009. – 368 с.

					КБ.КР.Б – 125 – 08 – ПЗ	Арк. 71
Змн.	Арк.	№ докум.	Підпис	Дата		

10. Белов Е. Основы информационной безопасности : учебное пособие для вузов [Текст] / Белов Е., Лось В., Мещеряков А. – М. : "Студио", 2006. – 356 с.
11. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: [учеб. пособие для вузов]. – М. : Горячая линия-Телеком, 2004. – 280 с.
12. 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.
13. SaM Solutions. Структура IoT системи [Електронний ресурс] / SaM Solutions. – 2019. – Режим доступу до ресурсу: <https://sam-solutions.by/industries/internet-veschey/>
14. Стандарт NB-IoT Low-Power and Wide-Area, LPWA [Електронний ресурс].– 2019. – Режим доступу до ресурсу:
15. [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](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).
16. 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.
17. NetSim Professional [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: <https://www.tetcos.com/netsim-pro.html>
18. Протоколи з'єднання з IoT [Електронний ресурс]. – 2019. – Режим доступу до ресурсу <http://www.rtsoft.ru/press/articles/detail.php?ID=2718>.
19. 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-rozgartannya-chetvertoi-promislovoi>.
20. Борейко О.Ю. Проектування IoT // електрон. текст. дані URL: <https://www.slideshare.net/ssuserf405bc/iot-79608563> (дата звернення: 04.12.2020)

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		72

21. Інформаційна безпека інтернету речей (Internet of Things) // електрон. текст. дані URL:
[http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_интернет_вещей_\(Internet_of_Things\)](http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_интернет_вещей_(Internet_of_Things)) (дата звернення: 06.12.2020)

22. 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)

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

24. 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](https://www.windriver.com/whitepapers/security-in-the-internet-ofthings/wr_security-in-the-internet-of-things.pdf) (дата звернення: 08.12.2020).

25. 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)

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

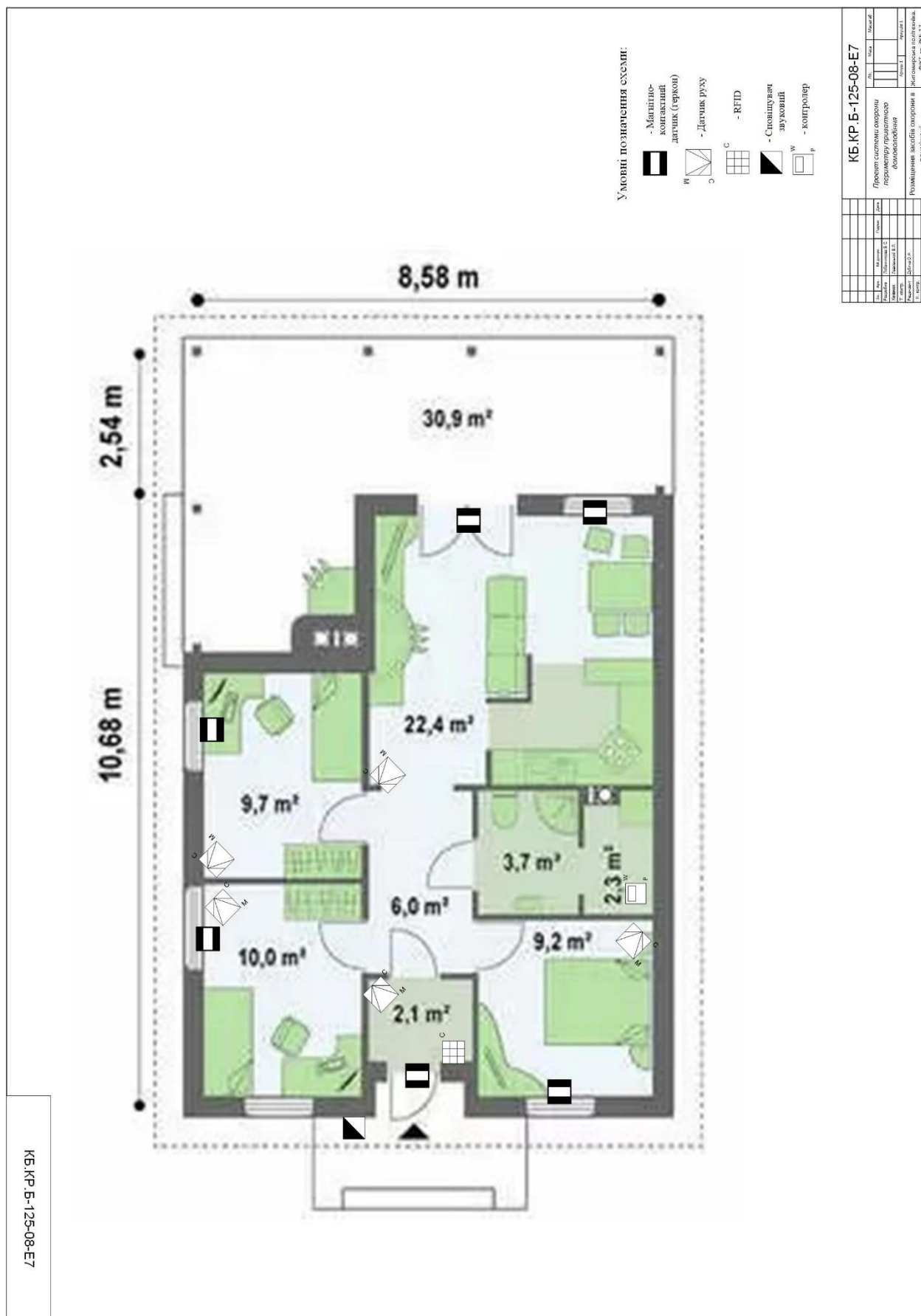
27. Туранська, О.С. Розвиток методів захисту інформації в безпроводових сенсорних мережах: магістерська дис.: 172 Телекомунікації та радіотехніка / Туранська Олена Сергіївна. – Київ: НТУ України «КПІ імені Ігоря Сікорського», 2018. - 67 с.

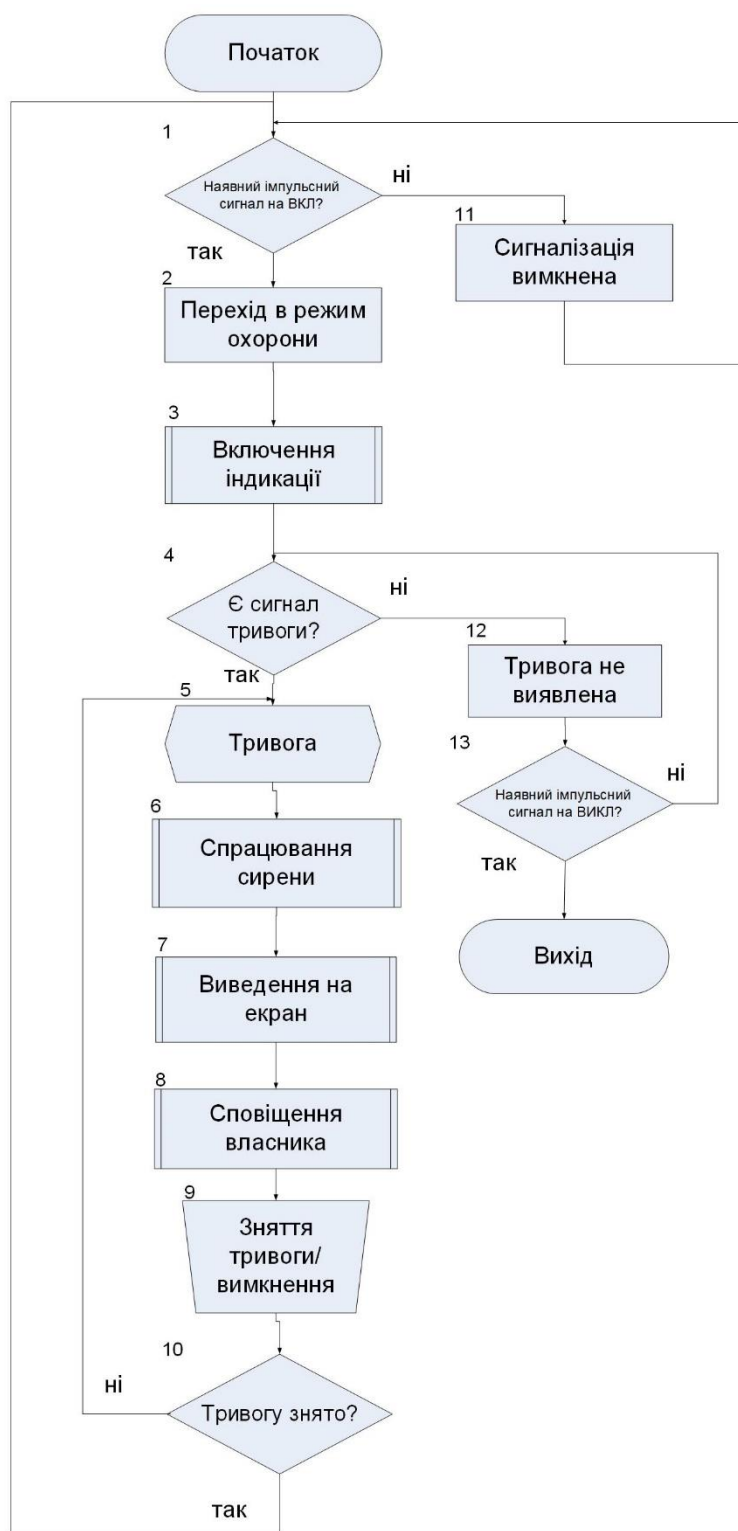
28. Корченко О. Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах / О.Корченко, М. Александер, Р. Одарченко, А. Наджи, О. Петренко // Захист інформації, 2016. – № 1. – С. 48-56.

ДОДАТКИ

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
						74
Змн.	Арк.	№ докум.	Підпис	Дата		

КРЕСЛЕННЯ





КБ.КР.Б-125-08-А2									
За	Внес	№ докум.	Листів	Дат	Проект системи охорони периметру приватного домогосподарства				
Розроб	Детальний 1				Лист	Мета	Місця		
Експерт	Детальний 2				Лист	Листів			
Т. експерт	Деталь 3				Власник має алгоритм функціонування системи				
Листів	Деталь 4				Нитомікський політехнік, ФІКТ, гр. 96-17				
Власник	Деталь 5								
Специфік	Деталь 6								

Змн.	Арк.	№ докум.	Підпис	Дата

ПУБЛІКАЦІЇ



Змн.	Арк.	№ докум.	Підпис	Дата

КБ.КР.Б – 125 – 08 – ПЗ

Арк.

79

Секція 2. Комп'ютерна інженерія та кібербезпека

- Інформаційна безпека в системах охоронного відеоспостереження
Дубина О.Ф., Дацюк А.О.
- Аналіз вірусних програм методами зворотної інженерії
Егоров С.В., Шкварницька Т.Ю.
- Програмний метод захисту операційної системи Windows на базі технології Blockchain
Ільєнко А.В., Ільєнко С.С., Куліш Т.М.
- Особливості безпечного підключення датчиків Інтернету речей до хмарного середовища Azure
Пулеко І.В., Топольницький П.П., Філіпов В.А.
- Аналіз останніх зловмисних дій у кіберпросторі
Романюк О.Н., Борисова К.О.
- Технології Edge computing при побудові IoT системи охорони периметру
Лобанчикова Н.М., Лобанчикова В.С.

ТЕХНОЛОГІЇ EDGE COMPUTING ПРИ ПОБУДОВІ ІoT СИСТЕМИ ОХОРОНИ ПЕРИМЕТРУ

Розвиток інформаційних технологій та входження людства в четвер-ту промислову революцію (INDUSTRY 4.0), призвело до виникнення ряду новітніх технологій, що стрімко входять у наше життя, зокрема технології Інтернету речей (IoT). Їх впровадження з кожним роком зростає величезними темпами. IoT-системи впроваджуються, як у побуті, так і у промисловості, в цілому у діяльності людини. Не обійшло впровадження такого роду систем і об'єктів критичної інфраструктури. Все це створило нові загрози кібербезпеки у житті людства, нові виклики та можливості. Наслідки вдалих кібератак можуть бути катастрофічними, як для окремого члена суспільства, так і для нації, людства в цілому.

Дослідження процесів захисту від кібератак в інформаційному суспільстві набирає обертів та розділяється в залежності від об'єктів захисту. Задача мінімізації кібернетичних впливів внаслідок атак на IoT-системи є актуальною задачею сьогодення. Найбільша кількість атак припадає на портативні (кінцеві) пристрої, використання безпроводних технологій зв'язку між елементами системи створює передумови для здійснення кібератаки на систему. Особливо актуально дана задача ставиться при створенні систем охорони периметру військових об'єктів, об'єктів критичної інфраструктури та інших об'єктів, де реалізація атаки може мати геополітичне значення.

Підходи до побудови IoT постійно удосконалюються, так само як і технології, методи та підходи до їх захисту. Поява технологій edge computing направлена на вирішення кола задач кібербезпеки, концепція якої базується на децентралізованому зборі та обробці даних, тобто найближче до кінцевих IoT-пристроїв. Використання такого підходу при побудові IoT-систем має ряд переваг, зокрема:

- мінімізація часу на обробку та прийняття рішення;
- зменшення навантаження на канали передачі даних;
- зменшення об'ємів даних, що зберігаються в хмарі чи на фізичних серверах;
- зменшення навантаження на центри обробки даних (ЦОД).

Комбінування IoT та edge computing в сфері кібербезпеки може використовуватися для:

- моніторингу безпеки мережі;
- аутентифікації;
- шифрування;
- виявлення порушень в системах охорони периметру та контролю доступу;
- інформаційних відеосистемах при аналізі потоку даних та розпізнавання;
- аналітики безпеки у питаннях виявлення зловмисного програмного забезпечення, компрометації IoT-пристроїв та їх захоплення;
- прогнозування загроз;
- захисту інтерфейсу,
- механізмів доставки.

Провідну роль у кібербезпеці IoT відіграє компанія Cisco, що розробила і запропонувала ряд концептуальних і технічних рішень щодо захисту та дослідження IoT-технологій, в тому числі і IoT-систем. Зокрема розроблено фреймворк безпеки IoT, що став корисним доповненням до еталонної моделі.

Набір датчиків, що використовується в системах охорони периметру є визначеним, однак на кожному об'єкті різняться їх комбінування, розміщення, налаштування. Типовими є датчик руху, камера відеоспостереження, перепустка та сирена. Їх кількість буде залежати від периметру зони охорони, однак вони є типовими для більшості систем охорони. Для дослідження процесів кібернападів, проведемо моделювання кластеру системи охорони в програмному середовищі Cisco Packet Tracer, що включає відеокамеру, датчик руху, сирену, RFID-зчитувач та RFID-картку, шлюз для прийому/передачі інформації та відповідно монітор IoT. Ці пристрої і є стандартними компонентами IoT-системи охорони периметру. 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, а також перевірено їх працездатність. Такого роду кластер використовуємо для моделювання та аналізу кібератак на такого роду системи, дослідження процесів відновлення системи після атак.

Така емуляція дозволяє розробити ряд практичних засобів щодо підвищення рівня кібербезпеки IoT-систем охорони периметру та безпосереднього впровадження на об'єктах захисту. Побудова комп'ютерна модель дозволяє нам визначити потенційні кіберзагрози та розробити технологію забезпечення кібербезпеки компонентів IoT.

Міністерство освіти і науки України
Житомирський державний технологічний університет
Національний технічний університет України
"Київський політехнічний інститут" ім. І. Сікорського
Тернопільський національний економічний університет
Харківський університет радіоелектроніки
Вінницький національний технічний університет
Житомирський державний університет ім. Івана Франка
Житомирський військовий інститут імені С.П. Корольова

ТЕЗИ ДОПОВІДЕЙ

I Всеукраїнської науково-технічної конференції

*Комп'ютерні технології:
інновації, проблеми, рішення*



м. Житомир, 19-20 жовтня 2018 р.

ЖДТУ
Вид. О.О. Євенок
2018

					КБ.КР.Б – 125 – 08 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		82

Секція 2. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА

Шестаков В. І.	Модель кібернетично-інформаційного циклу роботи ситуативного комплексу управління	65
Констанчук В.О., Ефремов М.Ф.	Що таке TELEGRAM-БОТ?	68
Олійник О.О.	Дослідження та аналіз алгоритмів на ринку криптовалют	70
Ефремов Ю.М. Герасимчук Є. С., Ефіменко А.А.	Особливості побудови системи життєзабезпечення об'єкту критичної інфраструктури з використанням технології «InternetOfThings»	72
Ізотов І.В., Сутоняк І.І.	Web-орієнтована система аналізу продажу будівельних матеріалів	74
Хабазія П.П., Сутоняк І.І.	Система геолокаційного позиціонування електронного каталогу фотографій	76
Кирилович В.О., Сутоняк І.І.	Веб-портал для аналізу ефективності SEO сайту	78
Бондаренко В.О., Олейник А.А., Субботин С.А.	Применение сверточных нейронных сетей в распознавания рукописных цифр	80
Пількевич І.А., Маєвський О.В.	Порівняльний аналіз шумозахищеності цифрових сигналів	82
Гіляновський А.М., Ефіменко А.А.	Віддалене керування освітленням через програмно-апаратний модуль системи розумний дім в мережі інтернет	84
Шпирко Р.В.	Безпека електронної комерції на основі протоколу TLS	86
Таралевич О.О., Лобанчикова Н.М.	Модель SCADA-системи клімат-контролю інфекційного відділення	88
Мельник А.О., Лобанчикова Н.М.	Модель комп'ютеризованої системи віддаленого управління припливно-витяжною установкою	90
Скоkun Я.П., Лобанчикова Н.М.	Інформаційна технологія візуалізації процесів управління камерами в'ялення риби промислового підприємства	92
Башинський Ю.М., Лобанчикова Н.М.	Інформаційна технологія ідентифікації співробітників організації	94
Годован В.В., Ставська В.С.	Шляхи удосконалення технологій інженерно-технічного захисту банкоматів	96
Косовець М.А., Товстенко Л.М.	Реалізація швидкісної системної магістралі для задач раділокації	98
Супрун В.О.	Підсистема бізнес-аналізу особистих фінансів на платформі Андроїд	102

ШЛЯХИ УДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ БАНКОМАТІВ

Сьогодні спостерігається інтенсивний ріст та розвиток банківських послуг та систем самообслуговування (банкоматів, платіжних терміналів). Як стверджують спеціалісти по банківським технологіям, зараз у всьому світі функціонує приблизно 1,4 млн. банкоматів різних типів. Сучасні банкомати стають все більш інтелектуальними та функціональними. Якщо перші моделі тільки могли працювати з магнітною стрічкою кредитних карт, то сучасні машини можуть обробляти «чипові карти», а також виконувати велику мисливну функцій. Сьогодні користувачі можуть здійснити за допомогою банкомату різноманітні платежі: поповнити рахунок мобільного оператора за жезу, сплатити комунальні платежі і т.д.

Однак для реалізації всіх цих можливостей необхідна надійна інформаційно-комунікаційна мережа, що відповідає за передачу даних.

У світі вже зареєстровано цілий ряд інцидентів, коли великі мережі банкоматів під управлінням Windows виходили зі строю, діючи комп'ютерним вірусом. У всіх випадках банкомати виявлялися відключеними від загальної інформаційно-комунікаційної мережі на декілька годин.

Таким чином мережі банкоматів можуть бути схильні до наступних видів загроз: вірусні атаки, зловмисні дії персоналу, помилки адміністратора та ін. Крім цього часто банкомати зосереджуються в неконтрольованих зонах, здійснюючи зв'язок з банком через публічні мережі.

На рисунку 1 показано проєкт модернізованої інформаційно-комунікаційної мережі. Умовні позначення: R_Scpi – центральний маршрутизатор (hub), що розташований у Центральному офісі; R_X – маршрутизатори, що розташовані у регіональних відділеннях банку; X – номер внутрішньої мережі регіонального відділення; SW_X – комутатори, X – номер комутатора; WS_X_Y – робочі станції операторів, X – номер внутрішньої мережі, Y – номер робочої станції.

При побудові модернізованої мережі за основу було взято загальну інформаційно-комунікаційну мережу XXX банку в Україні. Перед безпосереднім налагодження захищеної ІКМ, було здійснено проєктування схеми мережі в середовищі-емуляторі GNS.



Рис.1. Проєкт модернізованої ІКМ

Проведення розробки та тестування програми функціонування підсистеми інженерно-технічного захисту банкоматів комерційного банку суттю якої є управління системою охорони банкоматів від несанкціонованого доступу на базі контролера MaxuConFlexu за допомогою спеціального програмного середовища в симуляторі роботи контролера «Конфігуратор FBD». Головне вікно програми, що відображається на екрані контролера, представлено на рис.2.



Рис.2. Вигляд головного вікна програми

За допомогою розробленої програми роботи контролер здійснює контроль за сигналами датчиків та проводить відключення сирени при виявленні сигналу тривоги.