**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувачка кафедри кібербезпеки
та захисту інформації
_____ Наталія ЛУКОВА-ЧУЙКО
“14” червня 2022 р.

# ПОЯСНЮВАЛЬНА ЗАПИСКА

## випускної кваліфікаційної роботи

***бакалавра***
(назва освітнього рівня)

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

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

**освітня програма** Кібербезпека
(назва освітньої програми)

**на тему:** «Удосконалення алгоритмів та принципів охоронних систем для захисту від кіберзагроз»

**Виконавець:** студент IV курсу, групи КБ-42

_____ **Павло ВЕРЕМЕНКО**
(підпис) (прізвище ім’я по-батькові)

| | **Прізвище, ініціали** | **Підпис** |
|---|---|---|
| **Керівник** | Яніна ШЕСТАК | |

| | | |
|---|---|---|
| **Нормоконтроль** | Юрій ЩЕБЛАНІН | |

**Київ 2022**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
“01” листопада 2021 р.

# ЗАВДАННЯ
## на виконання дипломної роботи (проекту)

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

**освітньої програми** Кібербезпека
(назва освітньої програми)

**студенту** **КБ-42** **Верменко Павлу Петровичу**
(група) (прізвище ім’я по-батькові)

**Тема дипломної роботи** Удосконалення алгоритмів та принципів охоронних систем для захисту від кіберзагроз.

**1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ**

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол № 5 від 29.10.2022 р.

**2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ**

рмаційні технології в охоронних системах, Ajax Pro, структура та модель роботи охоронних систем, технології забезпечення інформаційної безпеки

**3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ**

Сучасні охоронні системи, програмні та апаратні засоби в охоронних системах, правова база в сфері охоронних систем, технології які використовуються для та побудувати для нього модель загроз.

**4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ**

**Практична цінність** Розроблені повноцінні рекомендації, які можуть бути використані, як для інтеграції готових рішень так і для створення власної

системи для охорони різних типів об’єктів.

**5. ДАТА ВИДАЧІ ЗАВДАННЯ**

Дата видачі завдання: 29.10.2021 року.

| | | |
|---|---|---|
| Завдання видав | _____ | Яніна ШЕСТАК |
| | (підпис) | (ім’я, прізвище) |
| Завдання прийняв до виконання | _____ | Павло ВЕРМЕНКО |
| | (підпис) | (ім’я, прізвище) |

**КАЛЕНДАРНИЙ ПЛАН**

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 29.10.2021 – 22.01.2022 | *виконано* |
| 2 | Аналіз літератури | 23.01.2022 – 09.02.2022 | *виконано* |
| 3 | Аналіз історії та розвитку охоронних систем | 10.02.2022 - 23.02.2022 | *виконано* |
| 4 | Аналіз побудови та інформація про типи охоронних систем | 24.02.2022 - 08.03.2022 | *виконано* |
| 5 | Збір відомостей щодо актуальних ППК та датчиків | 09.03.2022 – 29.03.2022 | *виконано* |
| 6 | Дослідження загроз для датчиків | 30.03.2022 – 19.04.2022 | *виконано* |
| 7 | Аналіз вразливостей в каналах зв’язку ППК | 20.04.2022 – 03.05.2022 | *виконано* |
| 8 | Створення рекомендацій по побудові та підключенню охоронних систем | 04.05.2022 – 17.05.2022 | *виконано* |
| 9 | Оформлення пояснювальної записки | 18.05.2022 – 29.05.2022 | *виконано* |
| 10 | Підготовка до захисту дипломної роботи | 01.06.2022 – 05.06.2022 | *виконано* |

| | | |
|---|---|---|
| Студент-дипломник | _____ | Яніна ШЕСТАК |
| | (підпис) | (ініціали, прізвище) |
| Керівник випускної кваліфікаційної роботи | _____ | Павло ВЕРЕМЕНКО |
| | (підпис) | (ініціали, прізвище) |

Термін подання дипломної роботи до ЕК 08.06.22.

# РЕФЕРАТ

Пояснювальна записка до моєї дипломної роботи на тему: «Удосконалення алгоритмів та принципів для захисту від кіберзагроз» складається зі вступу, основної частини (до якої відносяться 3 розділи), Висновку та списку літератури і джерел. Загальний обсяг роботи – 50 сторінок. Робота містить 14 рисунків. Список використаних джерел включає 18 джерел.

**Об'єкт дослідження** – алгоритми та принципи роботи Охоронних систем

**Мета роботи** – дослідити та розробити рекомендації щодо підбору та взаємодії з охоронними системами.

**Предмет дослідження** – методи та способи усунення загроз у охоронних системах.

**Метод дослідження** – аналіз охоронних систем та існуючих засобів для подолання інформаційних загроз.А також аналіз літератури і документів та порівняння.

**Практичне значення роботи -** полягає у створенні практичних рекомендацій для побудови, налаштування та удосконалення охоронних систем.

Результати здійснених у дипломній роботі досліджень можуть бути використані спеціалістами з побудови охоронних сигналізацій та при подальшому проведенні науково-дослідницьких робіт.

**Напрямки подальших досліджень:** розширення охоронних систем, їх поліпшення за допомогою поєднання з технологією «Розумний будинок»

**Ключові слова:** Охоронні системи, Датчики, шифрування, безпека, вразливість, алгоритми.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

| | | |
|---|---|---|
| API | – | Application Programming Interface |
| ІЧ | – | інфро-червоний |
| МК | – | магніто-контактний |
| ППК | – | прилад приймально контрольний |
| БОС | – | блок обробки сигналів |
| ПІЧ | – | пасивний інфра-червоний сповіщувач |
| РХ | – | радіохвильовий |
| ПЦС | – | пульт централізованого спостереження |
| ОС | – | охоронна система |
| КЗ | – | канали зв’язку |
| GSM | – | Global System (or Standard) for Mobile |
| ПЗ | – | програмне забезпечення |
| AES | – | Advanced Encryption Standard |

ЗМІСТ

# ВСТУП

**Актуальність** даної роботи пов’язан з тим, що характерною рисою нашого непростого часу є стрімке погіршення криміногенної ситуації в країні, тому злочини проти власності є більшою частину всіх злочинів які відбуваються у світі. У цьому випадку не варто розраховувати на оперативність правоохоронних органів, а відповідальність щодо їх безпеки та збереження свого майна люди змушені брати на себе.

Проте в нашій країні існує цілий ряд професійних організацій, які спеціалізуються на системах і заходах безпеки будь-якої важливості та специфіки

Привітність інформації дозволяє звести до мінімуму вплив від будь-яких нещасть, а головне – зберегти життя людей та їхнє майно. Ця проблема вирішується шляхом використання охоронних систем: сигналізації

Для вирішення проблем безпеки приватних осіб, будинків, підприємств на ринку представлений широкий спектр сучасних пристроїв, які надійно захищають непроханих гостей: будинок, офіс, гараж чи будь-який інший об'єкт. Однак високонадійне, але неправильно встановлене технічне обладнання не здатне захистити майно. Отже, щоб забезпечити повну безпеку недостатньо, щоб обладнати будинок або офіс складною і дорогою електронікою, необхідно також дотримуватися ряду кроків і правил повсякденного життя, виконання яких не є надтяжким, а встановлення сигналізації слід довіряти справжнім фахівцям своєї справи.

На сьогоднішній день стрімко розвиваються технології, що дозволяють створювати все більше систем, які попереджають події які пов’язані з небезпекою для майна або сповіщають про намагання злочинця щось зробити, попереджуючи саме правопорушення.

Починаючи від катастрофічних дарів природи, які несуть в собі ряд жахливих наслідків, звичайних крадіжок з наших будинків, які можуть бути для людей

фатальними, тому що грабіжник може вкрасти все те, що люди намагалися накопичити протягом життя.

А також ми можемо розглядати це не як майно, а як наприклад крадіжку цінної інформації іноземними диверсантами та спецслужбами, шкода від якої може завдати неприємностей будь-якого плану усій країні.

При розробці будь-якої системи безпеки всі технічні рішення повинні відповідати вимогам екологічних, санітарно-технічних, протипожежних та іншим нормам, що діють на території України, та забезпечувати безпечну для життя і здоров'я експлуатацію об'єкта.

У наш непростий час різні охоронні пристрої для захисту периметру приватного будинку, все більше набирають популярності, в більшості випадків це навіть життєво необхідно. На питання, що таке охоронна сигналізація периметру та з чого вона складається ми розглянемо в цій роботі [1].

# РОЗДІЛ 1
# ОХОРОННІ СИСТЕМИ: ІСТОРІЯ ТА ПРИНЦИП ПОБУДОВИ

## 1.1 Історія створення охоронних систем, їх розвиток

Важко повірити: перша у світі електромагнітна сигналізація вже була запатентована 21 червня 1853, який зображений на (рис 1.1), на ім'я Огастес Рассел Поуп, винахідника з Сомервілл в Бостоні. До того часу люди в основному покладалися на гучну балаканину своїх уражених гусей, цілісність своїх сторожових собак або механічний дзвін, щоб впіймати зловмисників на своїй власності [3].

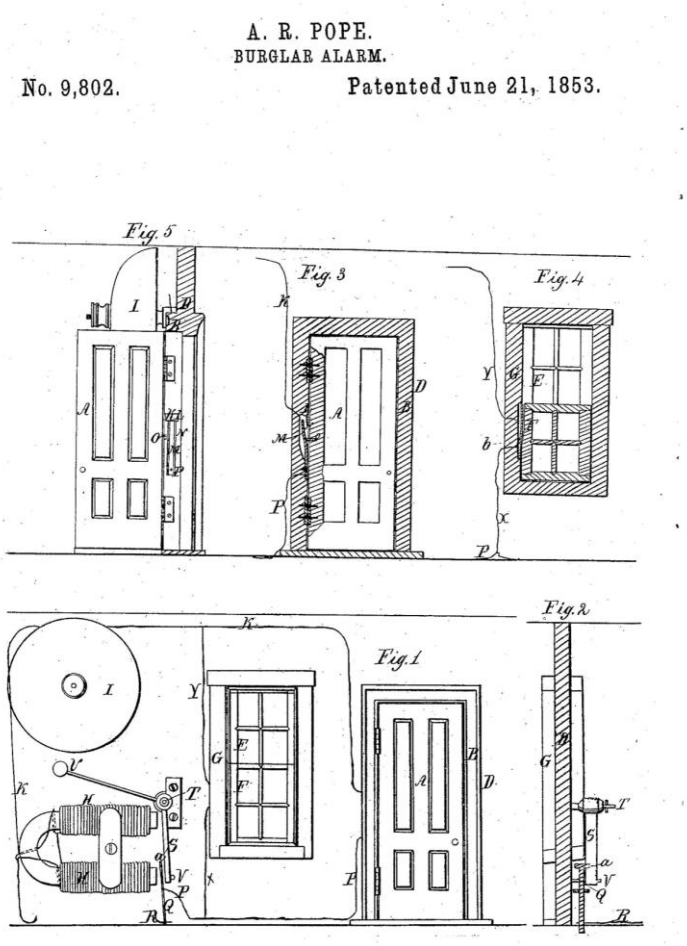
A. R. POPE.
BURGLAR ALARM.
No. 9,802. Patented June 21, 1853.

Рисунок 1.1 - Схематичний макет сигналізації Поупа

Гаджет Поупа з батарейним живленням може здатися дуже простим з сьогоднішнім поглядом на сучасні системи, але він виявився надзвичайно

ефективним проти зловмисників. Він відреагував на закриття електричного ланцюга: двері та вікна були з'єднані як незалежні блоки паралельним ланцюгом. Якщо двері або вікно були відчинені, а електричний ланцюг зачинений, раптовий потік струму призводив до вібрації одного з прикріплених магнітів у системі. Електромагнітні вібрації передавалися на молоток, який потім вдарився об мідний дзвін. Особливістю винаходу Поупа було те, що сигналізацію не можна було відключити просто закривши вікна або двері. Пружина перемикача, встановлена в стіні над дверима, також утримувала струм, щоб дзвінок міг продовжувати дзвонити.

Незважаючи на новаторську роботу Поупа, більшість людей зазвичай припускають, що хтось інший був батьком сучасної системи сигналізації. А саме Едвін Холмс, проте він був бізнесменом та засновником першої компанії з виробництва електричних систем сигналізації, яка фактично купила права на винахід Поупа у 1857 році. Саме він лідирував у бізнесі технології електромагнітної сигналізації зі своєю "Holmes Electric Protection Company" [4].

Холмс не був таким самим креативним інженером як Поуп, але виявився проникливим стратегом. Він набагато випередив свій час, коли справа дійшла до реклами. Щоб протистояти поширеному страху і скептицизму щодо електрики в 19 столітті, він опублікував імена відомих клієнтів у журналі New Yorker, які були готові довіритися своїй системі сигналізації. Щоразу, коли він друкував рекламу, вона завжди була разом із фотографією його «телеграфа охоронної сигналізації» і завжди одним і тим самим підписом. Холмс інстинктивно дотримувався принципів сучасного маркетингу, тому винахід Поупа поступово став брендом Холмса.

В той час довіра і захоплення людей у телеграфі також використовувалися Холмсом у ділових цілях двома способами: по-перше, у назві продукту він використав термін «телеграф» , а також у технічному використанні численних патентних прав на ізоляцію телеграфних дротів.

Холмсу не потрібно було багато уяви, щоб використовувати патент на будівництво центральної станції, куди могли б сходитися атмосферостійкі телеграфні кабелі його систем сигналізації. Щоб кабелі сигналізації своїх клієнтів

проходили через місто до його офісу, Холмс переїхав на верхній поверх будівлі в центрі Нью-Йорка. Незабаром відомі ювелірні магазини, такі як Tiffany або Lord & Taylor, вже були приєднані до його мережі.

Але найбільшого перевороту для компанії було досягнуто його сином Едвіном Т. Холмсом. Йому спала на думку ідея використовувати невикористовувані телефонні лінії підприємств у Бостоні вночі для власних систем сигналізації. Після величезного успіху цієї системи в Бостоні Холмс встановив тісні контакти з телефонною компанією і незабаром отримав ексклюзивне право використовувати нью-йоркську телефонну мережу для своїх систем сигналізації з добре налагодженими і підключеними лініями.

Ще одна віха в історії сучасних систем сигналізації була зроблена після Холмса молодою людиною на ім'я Едвард Калахан. Одного разу вночі бідолаха був захоплений зненацька у своєму будинку грабіжником і серйозно пограбований. Шокований інцидентом, Калахан почував себе зобов'язаним захистити свого себе від таких небезпек у майбутньому.

Його план полягав у тому, щоб помістити кожного із п'ятдесяти сусідів у безпосередній близькості від будинку Ендрю за допомогою однієї аварійної телефонної коробки та одного дзвінка, а потім з'єднати будинки один з одним. Для кожної телефонної скриньки домашнього господарства було визначено певну кількість дзвіночків, які можуть розрізняти будинки у разі крадіжки зі зломом. Якби в будинку А задзвонила сигналізація, будинки В і С знали б, що будинок А, ймовірно, був пограбований.

Поки він працював над першим апаратом екстреного виклику, Калахан мав ще одну вирішальну ідею: у містах особливо часто відбувалися крадіжки зі зломом - якщо його система не тільки спрацьовувала сигналізацію, а й надавала послугу, то була б необхідна аварійна центральна станція, яка могла б реагувати на вхідні заклики про допомогу. Він почав з поділу Нью-Йорка на райони, які мали бути підключені до центральної станції моніторингу. У разі екстреного виклику, що входить, буде відправлений кур'єр, щоб оперативно організувати допомогу для цього конкретного району. Перевага телефонних скриньок полягала в тому, що вони

вимагали невеликого обслуговування. Вони працювали на магістралі із місцевої центральної станції. У 1871 Калахан допоміг створити компанію American District Telegraph (ADT). Компанія була дуже успішною і займала офіси в Брукліні, Нью-Йорку, Балтіморі, Філадельфії та Чикаго з 1875 року.

Екстрені телефонні дзвінки Калахана стали стандартним використанням для поліцейських та пожежних служб, а також для кур'єрських служб. До кінця 1870-х років дві третини всіх проданих акцій було зроблено через цю систему.

### 1.2 Аналіз охоронних систем, їх будова

Зазвичай, системи охоронних сигналізацій, які представлені на нашому ринку, встановлюється для запобігання несанкціонованого проникнення (або спроби проникнення) на об’єкти. Залежно від типу оповіщення, воно або зупиняє злочинця від виконання плану злочину, або допомагає затримати його на місці злочину до прибуття відповідних служб.

Окрім цього охоронні сигналізації за останній час багато змін відбулося в цих системах, і виникло багато підтипів систем.

В цьому підрозділі ми роглнянемо основні типи, на які поділяють охоронні системи, та які їх ключові влаастивості.

Охоронні сигналізації поділяються на:

- За способом зв’язку в системі: дротові та бездротові (рисунок 1.2).


Рисунок 1.2 - Типи охоронних систем.

- За типом виконавчих пристроїв – на активні та пасивні (рис 1.3).


Рисунок 1.3 - Види охоронних систем  за типом виконавчих пристроїв.

Завдання активних систем - відігнати злочинців або утруднити їм проникнення в будинок, найчастіше вони оснащені сиренами, рідше - генераторами туману або електроімпульснити пристоями. Пасивними, зручніше захищати квартири, приватні будинки, комерційні об'єкти, і не бути поміченим правопорушниками для передачі сигнальної інформації. Крім того, системи зазвичай класифікують за такими критеріями: Залежить від того, кому надіслано повідомлення– автономні та пультові (рис 1.4)


Рисунок 1.4 - Класифікація охоронних систем

- Автономні:

Це сповіщення, яке надсилає сповіщення власнику. Перевага цього рішення полягає в тому, що ви платите лише за установку системи. Але якщо спрацює сигналізація, власнику доведеться виїжджати на місце злочину, викликати на допомогу сусіда або викликати поліцію. Це мінус, і це серйозно:

• Пультові:

Дистанційна сигналізація підключена до PCS - центральної станції моніторингу охоронної компанії, на яку надсилаються повідомлення. Отримавши сигнал, група фахівців вирушила на об’єкт, де встановили сирену. перевага:

- Швидка реакція дозволяє затримати зловмисника до того, як він завдасть серйозної травми власнику;

- Експерти легко впораються зі злочинцями;

- Поважна компанія несе фінансову відповідальність перед своїми клієнтами і зобов'язана відшкодувати їхні збитки, якщо вони не відреагують своєчасно.

Але не всі системи підтримують підключення до АРС, і ви повинні платити щомісяця за цю послугу.Окремо зараз виділяють ще 3тю групу *«GSM-сигналіза*ція»

Найпоширенішими останніми роками є сигналізації, де передача тривоги здійснюється за допомогою технології стільникового зв’язку.

GSM сигналізація являє собою систему з вбудованим GSM модулем і слотом для SIM-картки в панелі управління (ППК). Можуть використовуватися різні стандарти передачі (GSM, WCDMA), телекомунікаційні протоколи та підтримка каналів передачі Інтернету. GSM-сигналізація може використовуватися як автономна, так і дистанційна, власник отримує сигнал на мобільний телефон у вигляді дзвінка, SMS, push-повідомлення протягом декількох секунд роботи.

Основним компонентом системи сигналізації є центральний (концентратор, пульт, приймач і пристрій управління). Він з'єднується та обмінюється сигналами з усіма іншими пристроями. Більш надійною вважається система двостороннього зв’язку, де концентратор не тільки отримує сигнали від датчиків безпеки, але також може періодично їх тестувати, щоб перевірити роботу. Також в систему входять:

- Датчики, які реагують на тривожні події. Системи охоронної сигналізації – це в основному датчики руху та двері (вікна). Зазвичай вони доповнюються датчиками, які детектують розбиття скла;

- Виконавчі механізми, такі як звукові та візуальні сирени (сигналізація), і модулі зв'язку (GSM, Wi-Fi), як правило, вбудовані;

- Пристрої керування - брелок, клавіатура, тривожні кнопки. Для управління також можна використовувати смартфон з мобільним додатком.

У бездротових системах, де відстань між панеллю управління і датчиком велика, для посилення сигналу використовуються повторювачі. Крім того, для роботи системи потрібні дроти для забезпечення живлення, а в дротових системах - навіть дроти для передачі сигналу. Іноді в системи охоронної сигналізації інтегруються датчики пожежі та потопу, елементи систем «розумного дому» та камери відеоспостереження.

Система оповіщення з набором датчиків для будинків, офісів, магазинів та інших об’єктів шляхом своєчасного сповіщення зацікавлених сторін про надзвичайну ситуацію. Найвищий рівень захисту доступний при використанні систем дистанційного керування, які підтримують різні канали зв'язку.

### 1.3 Стандарти які використовуються в охоронних системах

Правила, стандарти та політика щодо зловмисників створені для того, щоб система була встановлена, обслуговувана й контролюється відповідно до стандарту, прийнятного як для поліції, так і для страхових компаній.

Важко говорити узагальнено тому, що більшість стандартів та правил не є утилітарними, а використовуються в різних країнах/компаніях, тому ми будемо в більшості говорити про Британські та Європейскі стандарти, так як вони є найбільш признаними та використовуються частіше за все.

Отже, головні та найвідоміші стандарти:

- PD 6662 Схема застосування європейських стандартів для систем сигналізації про вторгнення та затримки у Великобританії.

- BS 8243 Встановлення та конфігурація систем охоронної сигналізації, призначених для створення підтверджених умов тривоги

- BS 9263 Системи охоронної та аварійної сигналізації – введення в експлуатацію, технічне обслуговування та дистанційна підтримка

- BS EN 50131-1 Системи сигналізації, Системи вторгнення та затримки, Специфічні вимоги до системи [5].

Усі системи аварійної сигналізації, встановлені в Європейському Союзі, повинні відповідати основним стандартам, щоб їх прийняли страхові компанії та могли викликати поліцію. Європейським стандартом, що застосовується до сигналізації про зловмисники та аварійної сигналізації, є серія EN50131.

Відповідно до стандарту BS EN 50131-1:2004, системи охоронної сигналізації мають бути класифіковані за рівнем безпеки в залежності від типу порушника, який, як вважається, може спробувати перемогти систему.

Передбачається, що страховики підтримують підхід до класифікації, і очікується, що з часом вони рекомендуватимуть певні класи систем через певні ризики приміщень.

Інсталятори та клієнти можуть керуватися рекомендаціями страховиків щодо мінімального класу, необхідного для системи, та обговорювати, чи варто вибирати вищий клас.

В рамках нових європейських стандартів існує чотири класи безпеки:

Перед отриманням класу – системи тестуються у п'яти лабораторіях на відповідність різноманітним правилам, нормам та вимогам.

Коли технологія відповідає не лише за майно, а й за життя людей, вона має бути максимально надійною. І було б безвідповідально покладатися лише на заявлені характеристики та авторитет виробника – необхідна кваліфікована, незалежна експертиза. На європейському ринку систем безпеки стандартом безпеки є EN 50131-1:2006.

Акредитовані лабораторії піддають охоронне обладнання певним випробуванням: на функціональність, на те, чи стійке обладнання до погодних умов, як воно протистоїть механічним перешкодам та зовнішнім електромагнітним полям.

Перевіряється якість радіозв'язку, і навіть можливість зовнішнього на роботу пристрою. Результати випробувань записуються та розглядаються органом із сертифікації. Якщо необхідні випробування були проведені, обрані правильні методи та документи оформлені належним чином, організація видає сертифікат і присвоює пристроям клас надійності.

Надійність системи безпеки визначається її здатністю протистояти зловмисникам з різним ступенем знань та обладнання. Що клас, тим стійкіша система безпеки. Є два застереження: Клас 4 рідко зустрічається в системах на масовому ринку , оскільки вимоги стандарту надзвичайно високі, а клас 3 може бути присвоєний лише провідним системам безпеки. Тому виробники сучасних бездротових систем безпеки можуть отримати клас 1, або клас 2.

Не вдаючись у конкретні технічні деталі, можна сказати, що класи відображають стабільність та масштаб системи безпеки:

- Grade 1. Система може протистояти недосвідченим зловмисникам. Вона захищає найочевидніші точки входу, наприклад, вхідні двері. Вона підходить для приміщень, які наражаються на мінімальний ризик пограбування і фактично не містять цінностей.
- Grade 2. Система може протистояти досвідченим зловмисникам із спеціальним обладнанням. Вона захищає двері, вікна та інші можливі точки проникнення. Підходить для квартири, будинку чи офісу.
- Grade 3. Система може протистояти зловмисникам із професійними навичками та знаннями, які використовують портативне електронне обладнання. Захищаються всі можливі точки проникнення, а також стіни та стелі. Підходить для великих комерційних об'єктів, таких як торгові центри.
- Grade 4. Система може протистояти професійним групам, які наперед планують напади та оснащені повним набором обладнання. Це підходить для об'єктів, які наражаються на найбільший ризик пограбування або терористичної атаки.

У той час, як класи присвоюються окремим пристроям, системи безпеки оцінюються як єдине ціле. Клас системи визначається за влаштуванням системи з найменшим балом.

Якщо тільки один охоронний сповіщувач сертифікований за класом 1, вся система безпеки буде оцінена за класом 1. Навіть якщо 100 інших охоронних пристроїв у тій самій системі отримали оцінку 3.

Як відбується процес оцінювання девайсів, для отримання системою Grade-у.

1. Виробник надсилає пристрій на тестування, щоб підтвердити його відповідність європейським стандартам.

2. Випробування проводяться на кількох пристроях, одержаних із заводу виробника. З іншого боку, під час сертифікації оцінюється процес виробництва партії устройств.

3. Перевіряються пристрої, придбані у будь-якого представника виробника.

Для підтвердження сертифікації щороку потрібно відправляти пристрої для повторного тестування, а також проходити аудит відповідності виробничого процесу.

Як будильник проходить Оцінку?

Акредитовані лабораторії, такі як TÜV SÜD та Intertek, проходять суворі процедури тестування аварійної сигналізації. Тестування триває кілька місяців, протягом яких оцінюються всі компоненти, включаючи панель керування, детектори руху (пасивні інфрачервоні датчики), контактні датчики дверей і вікон, а також дзвінок.

Тести, які проводять перед наданням Grade-у системі або датчику:

1 – Загальні випробування

Загальні тести розглядають основні функції системи, як-от його здатність постановки та зняття з охорони, надсилання сповіщення та реагування на тривоги.

2 – Функціональні тести

Друга група тестів - це функціональні тести і зосереджені на датчиках тривоги. Проходження цих тестів означає, що система може визначити, який тип

тривоги: чи тривога викликана зловмисником, несправністю аппаратного елементу, низьким рівнем батареї в одному з пристроїв чи чимось іншим.

3 – Тести проти несанкціонованого доступу

Вони перевіряють здатність системи виявляти та реагувати на втручання, яке може мати кілька форм:

- глушіння сигналу
- перехоплення пакетів
- намагання втрутитись в аппаратну частину

4 – Фізичні випробування

Фізичні тести вимірюють стійкість сигналізації до фізичного впливу. Наприклад, такі, як сухе тепло, холод, пара, дим, пил і сонячне світло. Також є тести для конкретного пристрою. Для датчиків вікон/дверей випробувальна установа перевіряє, що несутєві удари не провокують систему на тривогу, як вібрація вантажівки, яка проїжджає повз.

5 – Випробування джерел живлення

Тут проводяться загальні тести аккумулятору – в основному його здатність пропрацювати достатньо тривалий термін при різних налаштуваннях сиситеми.

6 – Тести з реакцією та записами

Ці тести оцінюють здатність сигналізації подавати сигнал у разі злому та зберігати історію подій. Лаборанти будуть дивитися на аппаратну частину сирен, їх гучність, тривалість і здатність протистояти втручанням [7].

**Висновки за розділом 1**

В цьому розділі ми почали з аналізу історії та етапів розвитку охоронних систем та компаній які створювали їх. Очевидно що за останній час через надзвичайно стрімкий розвиток був зумовлений в цілому розвитком всіх сучасних технологій. Але цей розвиток, окрім того, що привніс багато нових функцій та спростив багато процесів в алгоритмах роботи системи, він надав системі багато вразливих місць, які можуть бути використані зловмисниками.

Так, як охоронні системи є надважливою галуззю, яка захищає життя, та майно людей – більше того, охоронні системи використовуються державою, навіть в таких вразливих галузях як: банкінг та воєнна інфраструктура, тому сертифікація достатньо серйозна, і дуже сильно градується від менш захищених до тих, що офіційно можуть бути встановленні в банківський сфері або навіть державних інституціях.

Також важливим фактором є велика взаємодія об’єктів інфраструктури з страховими компаніями (більше в країнах ЄС так північній Америці). До прикладу компанії, що займаються страхуванням, не можуть підписати договір з власником об’єкта де встановленна охоронна система нижче Grade 2.

Виробнику потрібна сертифікація своїх пристроїв. Тільки так система безпеки може на рівних конкурувати на масовому ринку та боротися за користувачів.

Сертифікація є складним завданням виробника. У стандарті EN 50131 наведено вимоги до всіх аспектів охоронного пристрою. Дотримуючись цих вимог, виробники не прогавлять двосторонній зв'язок між пристроями системи, шифрування даних або фізичну стійкість до впливу природи, вандалізму та злому. Це змушує виробників шукати та знаходити рішення та підштовхує їх до створення дійсно надійного продукту. І хоча несертифіковані технології нічого не винні грати за цими правилами, зворотний бік у тому, що можуть вийти з ладу будь-якої миті.

# РОЗДІЛ 2
# ВРАЗЛИВОСТІ В ОХОРОННИХ СИСТЕМАХ

## 2.1 Вразливості в охоронних системах

Логан Лемб, дослідник безпеки в Oak Ridge National Lab, та Сільвіо Чезаре з Qualys (компанії-постачальника хмарних послуг), провели незалежні вивчення охоронних систем безпеки.

У дослідженні Лемба було досліджено системи сигналізації, вироблені компаніями ADT та Vivint. Виявилось, що помилкові тривоги можна створити на відстані до 220 метрів з використанням системи радіозв'язку з можливістю програмування «USRP N210». Відключення аварійного сигналу вимагатиме відстані до 3 метрів від будинку.

Кожна система сигналізації, незалежно від марки, спирається на радіочастотні сигнали, що передаються між дверними та віконними датчиками та панеллю управління, яка викликає тривогу, коли відбувається вторгнення. Тим не менш, дослідники виявили, що системи не в змозі зашифрувати або ідентифікувати сигнали, що надсилаються від датчиків до панелі управління. Тому хакери можуть легко перехопити дані, розшифрувати команди та відтворювати їх для панелі керування.

Для того, щоб детальніше розібратись, як можна «обманути» охоронну сигналізацію ми розберемось на кожному кроку, де може відбуватись маліпуляція, та на кожному кроці будемо аналізувати як можна покращити систему, для поскладнення подібного підроблення інформації.

Які пункти ми розглянемо:

- Датчики (сповіщувачі)
- Зв’язок між датчиком та централлю
- Оповіщення (в залежності від типу системи ми розглянемо 3 різних варіанти)

## 2.2 Недоліки та вразливості в датчиках

Основні датчики охоронної системи: відкриття, руху та розбиття. Завдання всіх датчиків – моніторинг та надсилання сигналу на контрольну панель, яка у свою чергу передає інформацію на пульт охорони. Сигналізація спрацює в тому випадку, якщо сигнал, який відправляє датчик в даний момент, буде відрізнятися від попередніх сигналів про стан певного показника.

- **Датчики відкриття**

Їх встановлюють на двері та вікна. За принципом роботи такі датчики називають магнітоконтактними. Вони складаються з магніту, який встановлюється на рухому частину, та геркона (герметизованого контакту), що знаходиться на нерухомій частині, зображено на рисунку 2.1. У режимі «під охороною» зв'язок магнітгеркон замикається. Якщо його силоміць розімкнути, миттєво подається сигнал тривоги.

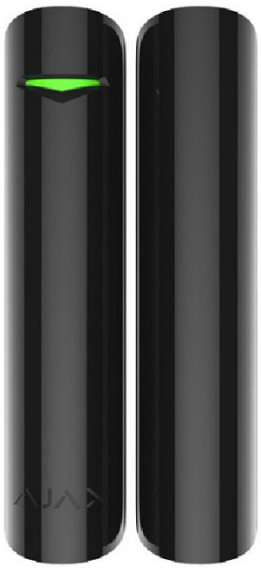

Рисунок 2.1 – Приклад магнітоконтактного датчику

Які недоліки спостерігаються в датчиках: зімітувати присутність магнітоконтактного зв'язку можна, приклавши до зовнішньої сторони дверей великий магніт. Насправді раніше данні датчики мали значно більше проблем в плані захисту від підлогу, проте зараз це виправлено появою тамперу.

Як охоронні компанії та користувачі захищенні від використання цієї вразливості:

Потрібно заздалегідь знати, на якій частині дверей точно знаходиться датчик відкриття.

Майже ніколи цей датчик не встановлюється окремо, він за принципом встановлення камер спостереження повинен перекриватися іншим датчиком (зазвичай руху).

- Датчики руху

За принципом роботи розрізняють два основні види: *інфрачервоний* та *ультразвуковий/радіохвильовий*.

*Інфрачервоні* датчики сканують простір на теплові випромінювання. По суті вони є датчиками температури Коли вмикається сигналізація, вони запам'ятовують показники температури у різних зонах приміщення та відстежують зміни. Якщо з'явиться новий об'єкт, що випромінює тепло, датчик зафіксує та надішле інформацію на контрольну панель. Приклад такого датчику зображено на рисунку 2.2

Рисунок 2.2 – Приклад інфрачервоного датчику руху

Які недоліки спостерігаються в датчиках:

Якщо  вдягти термокостюм (наприклад, костюм пожежного), що не пропускає температуру тіла людини поза його межі. (в такому випадку датчик не зможе задетектувати переміщення тепла в просторі)

Як охоронні компанії та користувачі захищенні від використання цієї вразливості:

Сам костюм теж має температуру, яка відповідає температурі навколишнього середовища, з якого зайшов зловмисник. Вона навряд чи збігається з температурою приміщення (наприклад, тамбур та квартира). Але якщо і уявити, що температура костюма разюче не відрізняється, то переміщення злодія по об'єкту все-одно порушуватиме показники теплових зон у різних точках однієї кімнати (наприклад, температура біля батареї вище, ніж навіть за метр від неї).

*Радіохвильовий та ультразвуковий датчики руху* відправляють і відстежують хвильовий сигнал, що повернувся. Новий об'єкт, що з'явився і рухається в приміщенні, порушуватиме хвильовий діапазон, і хвилі відправлені не будуть відповідати хвиль прийнятим. Приклад такого датчику зображено на рисунку 2.3

Рисунок 2.3 – Приклад радіохвильового датчику

Які недоліки спостерігаються в датчиках:

Якщо рухатися із швидкістю до 10 см/сек датчик не здатен задетектувати тривогу.

Як охоронні компанії та користувачі захищенні від використання цієї вразливості:

Рухатись з такою швидкістю на грані можливого, так як це повинна бути швидкість не людини в цікому, а швидкість найменшої теплової плями на тілі людини.

З такою швидкістю далеко не втечеш, та й часу у грабіжників не так уже й багато.

Професійне встановлення таких датчиків визначає необхідну висоту, кут нахилу та місце розташування для максимального охоплення території. Додаткові налаштування потреб клієнта можуть виключати реакцію на тварин, залежно від їх розміру і ваги.

Але захист від тварин породив занадто багато нових вразливостей в датчиках руху, так як вони в основному зроблені таким чином, що в датчику знижується чутливість (всієї зони покриття, або окремої її частини, зазвичай та що найближче до підлоги). Також, наприклад в вуличних датчиках це реалізовано таким чином, що з нижню полосу детекції датчик взагалі ігнорує якщо на верхній не помічено жодних змін. Це зроблено виробниками обладнання для покращення системи від хибних спрацювань, що як ми вже дізналися також оцінюється при наданні системі відповідного рівня (Grade-у).

Під час мого практичного вивчення цього питання був помічений дуже цікавий момент – вуличний датчик руху більш ніж за 200у.о від найвідомішого виробника на нашому ринку, не детектував зовсім мого племінника, так як його зріст менше ніж висота встановлення за інструкцією.

Але при цьому важливо враховувати, що різні датчики руху мають різну рекомендовану висоту встановлення, і відповідно від системи до системи різні умови встановлення на об’єкті  призводять до різних наслідків в вигляді різних безпековизх прогалин.

- Датчики розбиття

Встановлюються, як правило, біля вікон. Такі датчики називають акустичними. Вони працюють на відстеження перепаду та характеру звуку. При фіксації послідовності «глухий→дзвінкий» надсилається сигнал про вторгнення.

Такий датчик не спрацює, якщо проникнуть у будинок, відчинивши двері, але сповістить про несанкціоноване проникнення, якщо буде розбите скло або впаде якийсь великий предмет у кімнаті. Приклад такого датчику зображено на рисунку 2.4.

Рисунок 2.4 – Приклад датчику розбиття

Які недоліки спостерігаються в датчиках:

Ну в першу чергу треба згадати про те, що дана технологія спрацює тільки на чисте (не заклеєне нічим) та, що набагато більш важливо не загартоване скло.

А також, варто звернути увагу що принцип спрацювання датчику полягає саме в поєднання звуку розбиття та падіння «глухий→дзвінкий» - тому, якщо під склом буде розміщений м’який предмет, який не дозволить склу створити достатній дзвінкий звук від падіння скла алгоритм не здетектує тривогу.

Як охоронні компанії та користувачі захищенні від використання цієї вразливості: Тут основним є правильне встановлення таки датчиків, тому що по суті при стандартному розміщенні сповіщувача, та планування об’єкту не дозволить заздалегідь проробити маніпулювання біля вікна.

Різні охоронні системи можуть включати в себе різні складники, це залежить від цілей власника, щодо захисту, розміру та локації об’єкту, тощо. Нижче перераховані основні складові охоронних систем:

- Сповіщувачі охоронні (датчики руху), датчики удару, датчики об'єму (датчик, що реагує на переміщення предмета в певному об'ємі; у разі проникнення в приміщення, датчик об'єму повинен оповістити про сторонній рух в приміщенні), магніто-контактні датчики, електро- контактні датчики
- Пожежні сповіщувачі (компоненти систем пожежної сигналізації, призначені для виявлення пожеж на ранній стадії їх розвитку шляхом моніторингу фізичних або хімічних явищ, пов'язаних з пожежею (дим, тепло, світлове випромінювання) та передачі сигналів на блоки управління пожежами): дим Освітлення фотоелектричний димовід фотоелектричний, детектор полум’я, тепловий максимум тощо.
- Прилад приймально-контрольний пожежний
- Сповіщувач звуковий
- Сповіщувач світловий
- Відеокамери, відеореєстратори
- Керуючий сервер
- Приймально-передавальні термінали
- Освітлювальні пристрої
- Генератори охоронного диму
- Аварійні сповіщувачі: (датчики) сповіщувачі затоплення, сповіщувачі витоку газів та інші)

### 2.3 Вразливості в ППК

Головною вразливістю бездротових систем безпеки прийнято вважати радіозв'язок. Вона легко глушиться апаратурою, яку можна придбати «на кожному кутку», а без радіозв'язку сигналізація позбавляється можливості протистояти зловмисникам. Отже, об'єкт стає беззахисним.

Наразі, становить багато питань:

1. Як «глушать» радіозв'язок?

Глушення - незаконне створення перешкод у радіоканалі. Його використовують, щоб перешкодити передачі тривог у бездротових системах безпеки. Пристрої для глушіння називаються генераторами перешкод або пригнічувачами сигналу, а в народі - глушилками.

Генератори перешкод працюють у певному радіусі на частоті пристрою, роботі якого необхідно перешкодити. Якщо частоти приладу та глушилки не співпадають, глушіння не позначається на роботі пристрою.

Глушення може бути націлене як на окремі датчики, так і систему безпеки в цілому.

Спроби глушіння трапляються досить рідко - до 5 випадків на рік на 20 000 об'єктів, що охороняються. Це пов'язано з тим, що квартирні крадіжки на обладнаних сигналізацією об'єктах займають трохи більше 2-х хвилин.

“Глушення у разі недоцільно, оскільки це лише затягує процес» - Сергій Юр'єв, технічний експерт охоронної компанії «Карабінер» [6].

2. Які бувають глушилки?

Генератор перешкод може "глушити" певний діапазон або бути широкосмуговим, саботуючи відразу кілька технологій зв'язку системи безпеки.

Наприклад, професійні системи безпеки для зв'язку використовують 5 частотних діапазонів:

- мережі стільникового оператора 2G/GSM (900/1800 МГц), 3G/UMTS (2100 МГц) та LTE (900/1800/2600 МГц, залежно від регіону та оператора)
- мережа Wi-Fi (2,4 ГГц) (зараз починають вже з’являтись 5 ГГц)
- радіозв'язок (868,0-868,6 МГц залежно від регіону)

Широкосмугові перешкоди, які можуть створювати перешкоди в роботі кількох мереж (наприклад, Wi-Fi GSM), це: Портативний або портативний - Маючи розміри з мобільний телефон і відносно низьку потужність, він запобігає передачі даних (при відсутності перешкод) на відстань 5-15 метрів. Стаціонарні – цей тип пристрою більш потужний і дорожчий.

Із зростанням цін зростає діапазон і кількість мереж, які вони можуть блокувати. Чим ширша смуга частот і більший радіус перешкод, тим більшою має

бути потужність генератора перешкод. Потужний глушник дуже гарячий, тому потрібне додаткове охолодження. Також чим нижча частота глушіння, тим більших розмірів мають бути антени генератора перешкод. Все це позначається на габаритах пристрою — глушилки з радіусом дії від 100 метрів (на відкритому просторі) мають значні розміри, потребують примусового охолодження та живлення 230В.

Саморобні - як правило, малопотужні глушилки, що діють на невеликій відстані. Для збільшення покриття глушіння потрібні дорогі широкосмугові підсилювачі, а створення такого обладнання передбачає спеціалізовані навички.

- Глушення GSM каналу

Глушення каналу GSM може бути успішним лише при слабкому рівні сигналу GSM. Впевнений сигнал заглушити практично неможливо через високу потужність передавача вежі стільникового оператора.

В сучасних ППК, навіть якщо всі канали зв’язку будуть обірвані, то після відновлення зв'язку всі тривоги будуть доставлені до користувача та охоронної компанії.

А також  та підключені до нього пристрої постійно вимірюють рівень шуму в радіоканалі на різних частотах.

Система безпеки реєструє глушіння, якщо рівень потужності шуму вище -70 дБм протягом 30 секунд (показники можуть відрізнятись у різних виробників обладнання). Після цього хаб автоматично надсилає повідомлення про глушіння всім користувачам та охоронній компанії. Щоб уникнути обриву зв'язку, хаб переключається на менш зашумлену частоту.

Якщо при цьому ППК втрачає зв'язок з датчиком або пристроєм, він надсилає відповідні повідомлення користувачам системи безпеки та охоронної компанії.

- Глушіння Wi-Fi

При глушенні ППК  продовжує працювати повноцінно через Ethernet і SIM-карту, якщо ці канали зв'язку використовуються.

Якщо при цьому інші канали зв'язку недоступні або не підключені, центральний пристрій втрачає зв'язок із сервером, який відбиває тривогу

користувачам системи безпеки та охоронної компанії. А система продовжує працювати в автономному режимі - реєструє тривоги датчиків і сповіщає про них сиренами

- Глушення GSM, Wi-Fi, Радіозв’язку

Генератор перешкод, здатний одночасно зашумити діапазони зв'язку 2G/3G/LTE, Wi-Fi і Радіозв’язок на значній площі (ще й з урахуванням стін, перекриттів та сигналів, що відображають об'єктів у приміщеннях) — габаритний і дорогий прилад, не доступний у вільному продажі.

І все ж, якщо грабіжники мають такий широкосмуговий генератор перешкод, система безпеки зареєструє високий рівень шуму на частотах, які вона використовує і відправить відповідні оповіщення користувачам та охоронній компанії через Ethernet (якщо підключений). У програмах (якщо такі доступні від виробника) буде видно, що підключення Wi-Fi та мереж 2G/3G/LTE неактивні. Якщо підключення через Ethernet відсутнє, хаб втратить зв'язок із сервером. Про що сервер повідомить тривогою користувачам системи безпеки та охоронної компанії.

Як захистити свою систему безпеки від перешкод

1. Встановіть концентратор у місці, де його неможливо легко підшукати, подалі від дверей та вікон. Під час встановлення пам’ятайте, що розташування концентратора повинно забезпечувати стабільний рівень сигналу для всіх пристроїв.

2. Використовуйте всі доступні канали зв'язку. Якщо ваша система підтримує SIM-картки двох різних операторів - коли Ethernet зникає, панель керування перемикається на SIM-карту. ППК активує другу SIM-карту, якщо дані передаються не через мобільний Інтернет. Професійній системі потрібно до 4 хвилин, щоб замінити SIM-карту (у середньому 17 хвилин для системи безпеки). Використання двох SIM-карт не запобіжить перешкод GSM (оскільки обидві SIM-карти використовують однакову частоту), але допоможе у випадку, якщо одна з SIM-карт перестане працювати з якихось причин. Наприклад, через збої з боку мобільного оператора.

Сповіщення з одним каналом зв'язку ненадійне, оскільки воно може перестати працювати навіть з природних причин - і система не сповіщатиме користувачів і

охоронні компанії про сповіщення. Наприклад, якщо на вашому рахунку SIM-карти закінчилися гроші або через збій з боку провайдера. Також, такі сповіщення легше зламати: просто перебиванням (глушінням) частоти GSM (якщо використовується лише SIM-карта), або обрив кабелю Ethernet (якщо використовується лише дротовий інтернет).

Якщо система безпеки має кілька каналів зв’язку, один є основним каналом, а другий резервним. Така система є більш надійною, тому що кілька каналів мають меншу ймовірність виходу з ладу одночасно, а в разі природного збою система продовжить нормально працювати. Чим більше каналів зв'язку, тим більше шансів на своєчасне сповіщення користувачів і охоронних організацій про загрози.

Канали повинні бути різних типів. Якщо в ПКП встановлено кілька GSM-модулів, а інших каналів зв’язку немає, вважається, що у вас є лише один канал. При глушенні частот GSM система буде відрізана від зовнішнього світу.

Також має значення, скільки часу витрачається на перемикання з одного каналу зв'язку на інший. У дешевих сигналізацій процес може зайняти десятки хвилин. При цьому пограбування квартири рідко триває понад 5-10 хвилин.

Це пов’язано з тим, що виробники обладнання часто економлять на виробництві ППК втановлють один стільниковий модуль (GSM) але декілька слотів під SIM-карти, що насправді є застарілою технологію, і зовсім не підходить до використання в охоронних системах.

Як правило, хмарний сервер — це зв'язуюча ланка між централлю та системою безпеки, що керує додатком. Він дозволяє контролювати всі аспекти роботи обладнання, перебуваючи навіть за тисячу кілометрів від об'єкта — через інтернет. До того ж, сервер забезпечує передачу інформативних пуш-повідомлень про службові події та тривоги.

У професійній системі хмарний сервер також контролює зв’язок із охоронним обладнанням та його продуктивність шляхом обміну інтерв’ю. Чим вище частота опитування - тим швидше сервер виявляє проблеми.та попередить користувачів та охоронну компанію.

Розглянемо на прикладі такої охоронної української компанії як Ajax

Окрім можливості управління хабом через програми та отримання пуш-повідомлень, хмарний сервіс Ajax Cloud відповідає за відображення актуальних даних про систему безпеки. Він регулярно (від 10 до 300 секунд, залежно від налаштувань) обмінюється інформацією з хабом, та актуалізує стан пристроїв у додатках Ajax.

Якщо хаб перестає виходити на зв'язок, сервіс Ajax Cloud відправляє тривогу користувачам та охоронній компанії.

3. Захисний пристрій і панель керування використовують надійну технологію зв'язку

У бездротовій системі безпеки обмін інформацією між панеллю керування та датчиками відбувається по радіо. Зв'язок має бути дуже надійним - навіть короткочасні перебої небажані (вони збільшують час передачі оповіщення), втрата зв'язку неприпустима (центральний, а потім користувач і охоронна компанія не знають про оповіщення).

Як правило, професійні системи працюють на частоті 433 МГц або 868 МГц і використовують цей діапазон частот для зв’язку між панеллю керування та датчиком, а не з використанням однієї фіксованої частоти. Це дозволяє системі автоматично змінювати робочу частоту в разі аварії або навмисної аварії.. Ця техніка називається стрибком частоти.

*Чому Wi-Fi не підходить для зв'язку між охоронними пристроями?*

У багатоквартирних будинках і офісах частоти Wi-Fi (2,4 / 5 ГГц) дуже шумні і перевантажені пристроями: комп'ютерами, смартфонами, технікою. Це призводить до втрати даних під час передачі – зазвичай це називають «побутові перешкоди».

Якщо мережеві пристрої об’єкта (маршрутизатори, маршрутизатори, ретранслятори) беруть участь у передачі даних через Wi-Fi, то стабільність їх роботи визначає ефективність системи безпеки

Wi-Fi має відносно короткий діапазон зв’язку — близько 150 метрів без перешкод. Обмеження усуваються шляхом розгортання багатокомпонентних мереж на місцях, але кожне нове посилання знижує надійність системи безпеки.

Яку радіотехнологію використовує Ajax?

Система безпеки Ajax використовує радіотехнологію Jeweller для зв’язку між концентраторами та пристроями. Він працює в діапазоні 868,0-868,6 МГц або 868,7-869,2 МГц (залежно від регіону) і постійно перевіряє рівень шуму в радіоканалі. Як тільки значення шуму перевищує ліміт, концентратор виявляє перешкоди, перемикається на нижчий рівень шуму та надсилає відповідні повідомлення користувачам і охоронним компаніям.

Jeweler сповіщає не більше ніж за 0,15 секунди, автоматично регулює силу сигналу, економить заряд акумулятора пристрою та забезпечує радіус дії до 2000 метрів.

4. Зв'язок з пристроєм

Зв'язок між охоронними пристроями буває одностороннім і двостороннім. У першому випадку датчик надсилає сповіщення та сервісні події на панель керування, яка не спілкується з датчиком. Панель керування не дізнається, чи перестає працювати пристрій (через вандалізм чи поломку пристрою), чи з’єднання втрачено. І не буде попереджати користувачів і охоронні компанії про порушення захисту.

У двосторонній системі безпеки контрольна панель і датчики обмінюються інформацією. Датчик передає сигнал тривоги до тих пір, поки ПКП не підтвердить його - немає ризику втратити тривогу в разі короткої перерви. Панель керування може змінювати налаштування пристрою, опитувати їх, перевіряти наявність та статус. Надійність такої системи в рази вище.

### 2.4 Які вразливості є в сучасних ПЦС

ПЦС – пульт централізованого спостереження. Це своєрідний інформаційний центр, куди стікаються всі події з об'єктів. Центр обладнаний спеціалізованими технічними засобами, інформацію з яких приймає та аналізує оператор.

ГОСТами визначено, що пульт централізованого спостереження – це самостійний технічний засіб (сукупність технічних засобів) або складова частина системи передачі сповіщень, що встановлюється в пункті централізованої охорони

для прийому від пультових кінцевих пристроїв або ретранслятора сповіщень про проникнення на об'єкти, що охороняються, та (або) про пожежу на них, службових та контрольно-діагностичних сповіщень, обробки, відображення, реєстрації отриманої інформації та подання її в заданому вигляді для подальшої обробки, а також (за наявності зворотного каналу) для передачі через пультовий кінцевий пристрій на ретранслятор та об'єктові кінцеві пристрої команд телеуправління. Тобто об'єктові прилади передають інформацію про стан об'єкта та події, що відбуваються на ньому (постановка на охорону, зняття з охорони, тривога, несправність, порушення електроживлення та ін.) на пульт централізованого спостереження, де відбувається обробка інформації та видача оператору відповідних повідомлень.

Сучасні ПЦС виконуються на основі комп'ютера та спеціалізованого програмного забезпечення. Також робота пультів централізованого спостереження може будуватися з урахуванням локальної обчислювальної мережі (ЛВС). Це, як зазначають експерти, забезпечує можливість прийому інформації різними каналами зв'язку, її передачу великому колу користувачів, а також максимально використовувати можливості сучасних інформаційних технологій.

Принципово важливий момент – канали зв'язку, використовувані передачі від об'єктового устаткування ПЦС інформації та даних.

Донедавна телефонна мережа була єдиною середовищем передачі інформації від пристрою сигналізації на ПЦС. Це робилося, як правило, одним із двох способів. У першому автодозвоні віддалений прилад дзвонив на ПЦС і передавав коди про тривоги спеціальними тоновими посилками. Головним недоліком такого підходу є те, що зловмисник може перерізати телефонний дріт і проникнути на об'єкт, що залишиться непоміченим. У другому способі проводиться постійний контроль цілісності лінії, і якщо виявлено порушення, вважається, що надійшов сигнал тривоги. Але щоб здійснити такий контроль, потрібно ставити спеціалізоване обладнання на кожній АТС, до якої можуть бути підключені прилади охоронної сигналізації. Це дорого і клопітно, а часом неможливо з урахуванням різнотипної апаратури АТС. Загальним недоліком обох методів є також те, що телефонні лінії на

всьому пострадянському просторі загалом низької якості, або тривожне повідомлення не доходить до ПЦС, або занадто часто трапляються помилкові обриви зв'язку. До того ж багато об'єктів просто не телефонізовані. Передача тривожних сигналів радіоефіру – зовсім інший підхід. Тут дроти не перекусиш. Але складнощів і тут вистачає. Систем радіомоніторингу на фіксованій частоті є досить багато, проте є кілька серйозних проблем:

- сильні радіоперешкоди, що є в умовах міста;
- перешкоди на шляху поширення радіохвиль (побудови, нерівний рельєф місцевості);
- віддаленість об'єктів від базової станції, у зв'язку з чим потрібне встановлення великої кількості ретрансляторів.

Станції моніторингу, що використовують стільниковий канал зв'язку, з'явилися останніми роками. Поштовхом став швидкий і потужний розвиток і розповсюдження стільникового телефонного зв'язку стандарту GSM, який став серйозним стимулом для створення нових систем, що використовують широкі можливості нових технологій. Стільникова мережа стандарту GSM-900/1800 забезпечує кращу якість зв'язку і вже розгорнуто у більшості міст Росії та країн СНД. Системи, що використовують GSM-зв'язок, дозволяють здійснити охорону будь-яких об'єктів, у тому числі і нетелефонізованих. Мережі GSM дозволяють також здійснювати аудіо- та відеоконтроль за допомогою сучасних телефонів (смартфони та КПК, оснащені модулем GSM). Це дозволяє бачити і чути, що відбувається на об'єкті, що охороняється. Використання GSM усуває необхідність розгортати свою мережу ретрансляторів - використовуються ретранслятори оператора GSM. Внаслідок цього можна брати під охорону об'єкт скрізь, де працює мережа GSM-оператора.

Якщо ж говорити про об'єкти, де утруднене або неможливе прокладання кабельної інфраструктури і єдиними комунікаціями є лінії електропередачі (дачі, гаражі, промислові або віддалені об'єкти, що не обслуговуються), то альтернативи стільникового зв'язку немає в принципі.

І, звичайно, дуже перспективним є використання нових протоколів та мереж 3G (третього покоління стільникового зв'язку з протоколом USSD), спеціально призначених для корпоративних клієнтів, – віртуальні корпоративні мережі передачі даних з імітостійкістю та захистом інформації.

Способи передачі даних у GSM-комплексах:

У GSM-900/ 1800 використовуються 4 канали (способи) передачі інформації: голосовий, SMS (Short Message Service – служба коротких повідомлень), канал передачі даних (DTMF) та GPRS-технології. Голосовий канал добре знайомий власникам GSM-телефонів, це той канал, яким зазвичай користуються для звичайних розмов по мобільному телефону. Канал передачі даних і GPRS призначений для з'єднання комп'ютерів між собою через стільникові телефони, виходу в інтернет. Канал SMS призначено для передачі коротких цифрових повідомлень (до 160 байт). SMS передбачає наявність центру обслуговування повідомлень, що належить постачальнику послуг стільникового зв'язку. Повідомлення від абонента надходить до центру обслуговування, а потім передається адресату. Технічно SMS-канал добре підходить для передачі від віддаленого охоронного приладу на ПЦС. Його переваги: повністю цифровий канал з контролем цілісності повідомлення, гарантує, що доставлене повідомлення не містить помилок; - Можливість зв'язку при низьких рівнях сигналів в умовах перешкод; – можливість збереження повідомлення в центрі обслуговування, якщо адресат недоступний, та доставка повідомлення після того, як адресат потрапляє до зони дії зв'язку. Однак реальність така, що в наших конкретних умовах повідомлення може бути доставлене із затримкою в кілька хвилин або навіть годин, нерідко випадки зникнення повідомлень. Це пояснюється тим, що повідомлення ставиться в чергу та обслуговується зі звичайним пріоритетом поряд з іншими повідомленнями інших абонентів та повідомленнями оператора зв'язку. Загальносвітова статистика стільникових операторів показує, що близько 6% повідомлень втрачається і не доходить до адресата. Безумовно, потрібно ще назвати протоколи GPRS і DTMF, які останнім часом стають все потрібнішими за ринком.

Використання голосового каналу також має свої переваги та недоліки. Тому найбільш просунуті виробники використовують у своєму обладнанні всі 4 формати зв'язку. І в разі виходу з ладу одного каналу відбувається автоматичне перемикання на інший канал.

Як влаштований ПЦС?

Насамперед слід підкреслити, що необхідною умовою надійної роботи ПЦС є його перебування в зоні сталого мобільного зв'язку стандарту GSM-900/1800.

Конструктивно ПЦС, як правило, складається з комп'ютера, модулів зі стільниковими терміналами, зарядних пристроїв, кабелів для міжмодульних з'єднань, кабелів сполучення з ПК.

Мікропроцесорний модуль з'єднується зі стільниковим терміналом за допомогою роз'єму. Зарядний пристрій та модуль сполучення з ПК підключаються до гнізда. Модуль сполучення з ПК підключається до COM-порту ПК.

Функціонал ПЦС залежить від програмного забезпечення. Ми наведемо якийсь необхідний, на думку експертів, перелік функціональних можливостей, які сучасний ПЦС має надавати користувачеві.

Насамперед це прийом повідомлень від об'єктових блоків. Цей процес може супроводжуватися звуковим та візуальним супроводом, розшифровкою та обробкою.

Наступна функція – ведення централізованої бази даних. Вона забезпечує клієнт-серверну архітектуру, а також розподілений доступ до бази даних з різних комп'ютерів мережі. Дуже корисною є така функція, як постійний моніторинг стану об'єктів та тестування охоронних об'єктів.

Слід також назвати такі функції, як зберігання та відображення планувань об'єктів, різних схем, описів об'єктів (в текстовому вигляді), номерів кодів доступу, подій та їх розшифровки, описів зон, ведення архівів прийнятих повідомлень та всіх подій, що відбулися на об'єктах. Зрозуміло, має бути можливість оперативно роздрукувати бази даних об'єктів, архіву подій як повністю, і фрагментарно.

Дуже важлива для організації пультової охорони функція – можливість протоколювати час прибуття групи реагування на тривожний об'єкт.

Добре, якщо ПЦС автоматично створює графіки та звіти про роботу пульта за певний період часу – ця функція значно підвищує зручність користування.

- Розглянемо на прикладі станції моніторингу *STAM-2 (Satel, Польща)*

Станція моніторингу STAM-2 польської компанії Satel складається з програмного забезпечення, материнської плати для отримання повідомлень з ППК та захисного апаратного USB-ключа. Материнська плата може бути встановлена в будь-який вільний слот PCI ПК і може працювати без комп'ютера за допомогою автономного джерела живлення. Програма моніторингу значно полегшує роботу оператора системи, автоматично вибираючи події, які потребують його втручання, надаючи перелік інструкцій у кожній конкретній ситуації, нагадуючи про незавершені завдання. STAM-2 може обслуговувати понад 50 000 користувачів, друкувати звіти про дії оператора системи OPS, повідомляти про системні події та автоматично відстежувати несанкціоновані зміни системних файлів.

ПК СТАМ-2 підтримує такі способи обміну даними з ПКП: прийом сигналів у вигляді SMS-повідомлень по телефонних лініях, IP-каналах, мережах GSM, а також по ефірі при наявності радіостанцій VISONIC. При цьому вибір плат, що встановлюються на ПК, залежить від вибраних способів передачі даних. В рамках однієї станції моніторингу STAM-2 може працювати до 16 з'єднаних між собою плат, що дозволяє регулювати кількість доступних телефонних ліній та IP-адрес.

Структурна схема STAM-2 зображена на рисунку 2.5

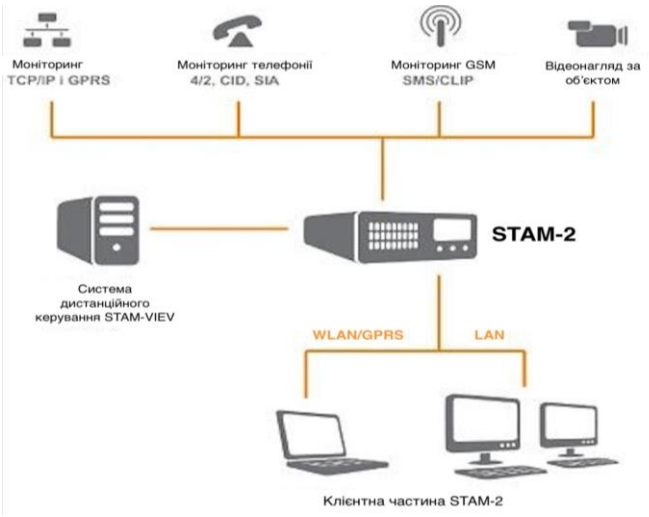


Рисунок 2.5 – Структурна схема системи STAM-2.

Система має модульний принцип побудови. Станція моніторингу STAM-2 польської компанії Satel складається з програмного забезпечення, материнської плати для отримання повідомлень з ПКП та захисного апаратного USB-ключа. Материнська плата може бути встановлена в будь-який вільний слот PCI ПК і може працювати без комп'ютера за допомогою автономного джерела живлення. Програма моніторингу значно полегшує роботу оператора системи OPS, автоматично вибираючи події, які потребують його втручання, надаючи перелік інструкцій у кожній конкретній ситуації, нагадуючи про незавершені завдання. STAM-2 може обслуговувати понад 50 000 користувачів, друкувати звіти про дії оператора системи OPS, повідомляти про системні події та автоматично відстежувати несанкціоновані зміни системних файлів.

ПК СТАМ-2 підтримує такі способи обміну даними з ПКП: прийом сигналів у вигляді SMS-повідомлень по телефонних лініях, IP-каналах, мережах GSM, а також по ефірі при наявності радіостанцій VISONIC.

Програмне забезпечення складається з кількох модулів, які забезпечують прийом та декодування інформації, відображення стану всіх об'єктів, підключених до системи, видачу тривожних сповіщень, фіксацію дій операторів при надходженні тривожних повідомлень, детальне подання кожного об'єкта; відображення журналу подій; контроль працездатності модулів зв'язку з концентратором.

Відповідні модулі ПЗ вирішують завдання з підготовки та ведення бази даних по об'єктах, програмування ключів перенесення даних для об'єктових приладів, забезпечують формування звітів по об'єктах та системі в цілому.

**Висновки за розділом 2**

За своєю сутністю ПЦС працює так само, як сервер які ми описували в минулому пункті – так само він зв’язується з пристроями через ППК, і так само, як і нові та більш професійні сервери охоронних компіній перевіряє зв’язок з всіма клієнтами.

Так само надійність отримання на ПЦС сповіщенн та тривог від датчиків (через ППК) залежить від каналів зв’язку які використовуються на охоронному центральному пристрою, але сам сервер охоронної компанії є менш надійним, через те що вони зазвичай використовують менш безпечні технілогії при підборі обладнання, та не завжди використовують хмарні сервіси в високим рівнем доступності в рік.

Тому часто охоронні компанії самі використовують резервні канали зв’язку, це може бути наприклад:

- резервний сервер на які події завжди дублюються, і в випадку атаки або обриву зв’язку по іншій причині система автоматично переналаштовується на отримання інформації з резервного каналу (серверу)
- налаштовують зв’язок по каналу Сервер виробника обладнання – власне ПО
- Використовують програмне рішення виробника, як резервний канал (по суті пряме використання серверних можливостей виробника, але тим самим прибирають вразливостей власного ПО і дозягаючи тим самим диверсифікації ризиків)

# РОЗДІЛ 3
# РЕКОМЕНДАЦІЇ ДЛЯ ПОБУДОВИ ОХОРОННОЇ СИСТЕМИ

## 3.1 Створення рекомендацій для побудови охоронних систем.

Отже, проаналізувавши багато статей, та вивчивши всі принципи, які впливають на «надійність» охоронної сигналазації, я можу надати певні рекомендації, які можуть бути використанні на практиці для побудови дійсно надійної (наскільки це можливо при сучасному стані розвитку технологій)

Розпочнемо ми з вибору типу системи:

На мою думку оптимальною зараз буде використання змішаної форми GSM сигналізації + за потребою за допомогою модулю інтеграції додати провідні датчики (цим також можна спросити побудову системи через, те що об’єкт може бути завеликий, або таке використання буде зручне на об’єктах з підземними приміщеннями) Для прикладу Multitransmiter від компанії Ajax, який зображений на рисунку 3.1, він дозволяє підключити до 18 провідних датчиків, які будуть також захищенні від знеструмлення.


Рисунок 3.1 - Модуль інтеграції Ajax Multitransmitter.

Конкретно розбирати типи використаних датчиків ми не будемо, бо це напряму залежить від типу та розміру об’єкту, що не дає змогу надати конкретні рекомендації.

Але на мою думку доцільним було б використання змішаних типів датчиків. Такі як датчики:

- Робиття + руху
- ІК + мікрохвильовий датчики руху в одному корпусі

Також, як було описано в другому розділі – вкрай важливим фактором є наявність в системі двустороннього зв’язку (ППК - датчики), для зменшення шансу на створення підлогу, або атаки типу «людина посередині».

Дані, що передаються між датчиками і централлю, повинні бути зашифровані і захищені від підлогу. Це дозволяє уникнути підміни частини датчиків - у гіршому випадку, брелока управління режимами охорони, оскільки зловмисники отримають повний контроль за системою безпеки.

Оптимально, якщо радіосигнал шифрується складним алгоритмом, тому що чим примітивніше шифрування, тим простіше зламати систему і отримати доступ до її управління. Наприклад, на злом 128-бітного AES шифрування необхідно витратити сотні років, а до сигналізації зі старим або примітивним шифруванням можна отримати доступ за допомогою кодграбер за лічені хвилини.

Замість стандартних алгоритмів та рішень часто використовують власні розробки. Всі дані, що передаються, шифруються AES алгоритмом з плаваючим ключем, наприклад. Кожний пристрій має індивідуальний ідентифікатор, а протокол передачі данних (зачасту це власна розробка і про них важко знайти деталі так як більшість компаній не розкривають деталі про принцип роботи та шифрування) передбачає систему властивостей та маркерів для ідентифікації своїх пристроїв. Систему безпеки не вдасться зняти з охорони пристроєм, що не прив'язаний до ППК (тобто тим, який не був до того зареєстрований в системі).

Більшість систем сигналізації сьогодні розгорнуті бездротовою мережею, що допомагає зменшити потребу в кабелях і складних процесах установки. Але хоча бездротові технології дуже зручні, їх ефективність повністю залежить від надійності

та стабільності можливостей бездротової передачі даних. Наприклад, щоб уникнути перебоїв у підключенні, система охоронної сигналізації Hikvision AX PRO використовує бездротові технології Tri-X та CAM-X, які забезпечують високонадійну передачу даних на надалекі відстані до 2000 метрів. У її панелі-концентраторі також використовуються подвійні радіочастотні чіпи та технологія частотного розширення спектру (FHSS) для блокування перешкод каналами та забезпечення одночасної передачі кількох попереджень безпеки.

Як ми зрозуміли в другому розділі – основна вразливість це канали зв’язку, тому для диверсифікації ризиків рекомендується використовувати як можна більше каналів зв’язку:

- Wi-Fi – на жаль більшість ППК ще не підтримують стандарт WPA3, але є і такі варіанти.
- GSM – бажано щоб і сім-карта і стільниковий модуль підтримували 4G+3G+2G, для усунення ризику, який ми розглядали в розділі 2.3
- LAN-порт – він завжди є основним каналом зв’язку, але з недоліків можна назвати тільки найвище енергоспоживання серед усіх каналів, і можливість фізичного обриву зловмисником.
- VHF – з’єднання

До прикладу можемо взяти девайс vhfBridge– це транспондер, що забезпечує хаб ще одним каналом зв'язку з пультом моніторингу. З модулем vhfBridge систему можна використовувати у містах з нестабільним інтернетом, горах, природно-заповідних зонах або пустельній місцевості.

vhfBridge дозволяє передавати тривоги та події системи завдки VHF-радіохвилям на десятки кілометрів. Він може використовуватись як основний або резервний канал зв'язку. Як на схемі такий канал виглядає зображено на Рисунку 3.2

Використовувати цю систему можливо в тому випадку, якщо об’єкти знаходяться на відстані до 10 кіломенрів від самої ПЦС, тому таке в нашій країні, на жаль, дуже не популярне. Але з багатьох причин цей метод зв’язку є вкрай корисним як резервний канал, так як він єдиний не спирається на жодне інтернет підключення (Ethernet/Wi-Fi/GSM зв’язок).

Налаштування такого каналу зв’язку є вкрай корисним для охоронних компаній, бо воно забезпечує найвищий рівень доступності для інформації, яка поступає з ППК до ПЦС.

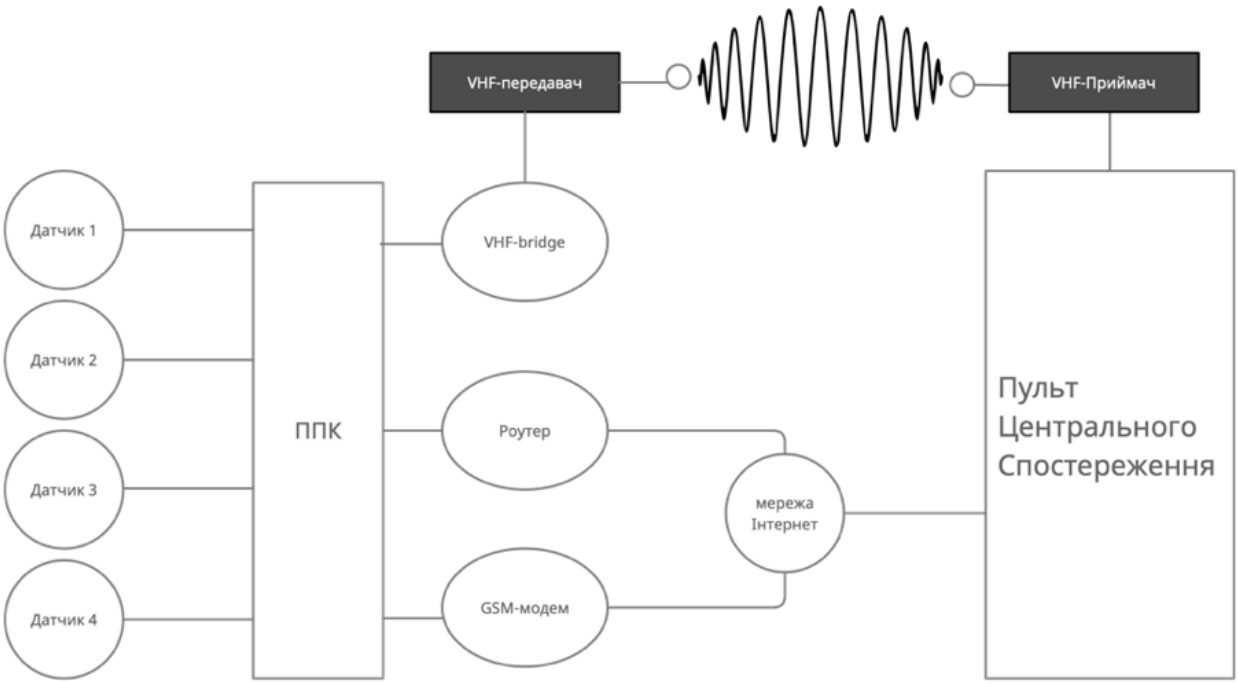


Рисунок 3.2 - Схема роботи ПЦС через VHF-bridge .

### 3.2 Рекомендації щодо побудови ПЦС

Є декілька рекомендацій для удосконалення актуальних ПЦС:
Важливим є налаштування резервних каналів зв’язку:
Резервний сервер на які події завжди дублюються, і в випадку атаки, або обриву зв’язку по іншій причині (це може бути будь яка спроблема з сторони інфраструктурного об’єкту на якому знаходиться Сервер, або сам ПЦС), система автоматично переналаштовується на отримання інформації з резервного каналу (серверу), як це працює ми можемо побачити на рисунку 3.1. На жаль, така система не використовується в вітчизняних компаніях, так як таке рішення є достатньо дорогим, і потребує більше фінансових та часових ресурсів.

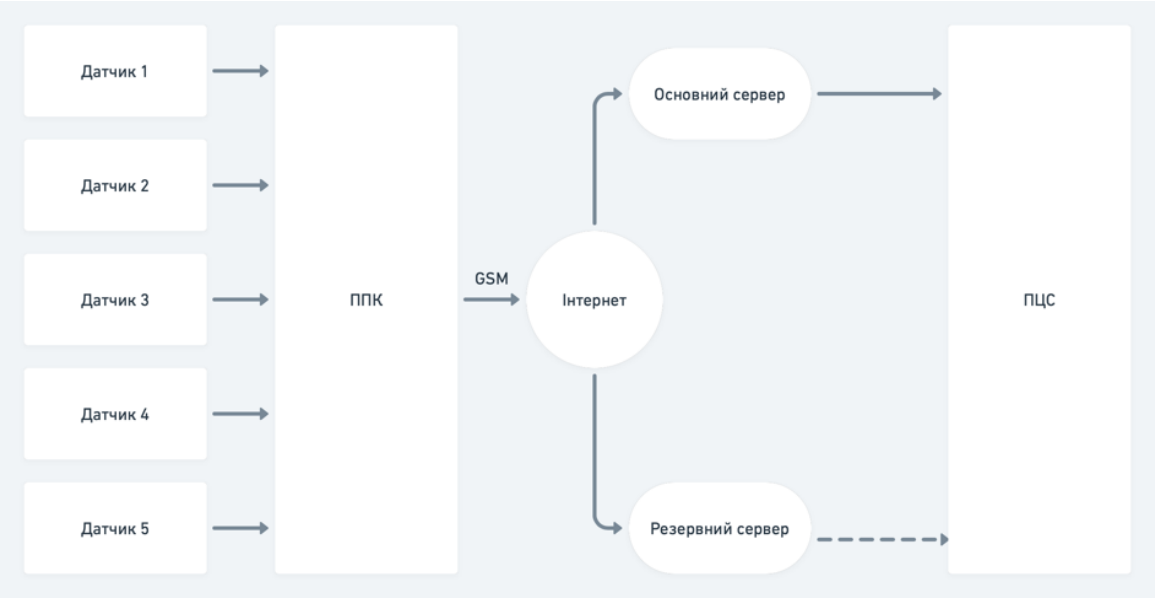


Рисунок 3.1 – Схематичне зображення резервного серверу.

В цьому випадку, ми не захищаємось від всіх вразливостей, що можуть бути присутні в серверній частині ПЦС, але в такому випадку після можливих проблем на стороні сервера ми не втрачаємо спроможність системи в цілому реагувати на події.

Також, важливим було б використання різних типів підключень (сервер - ПЦС), але на жаль, часто при використанні сучасних ПЦС, ми спостерігаємо наявність тільки старої технології Socket, хоча вона застаріла і з нею присутні багато проблем.

Налаштовування зв'язку по каналу «Сервер виробника» – власне ПО, як зображено на рисунку 3.2.

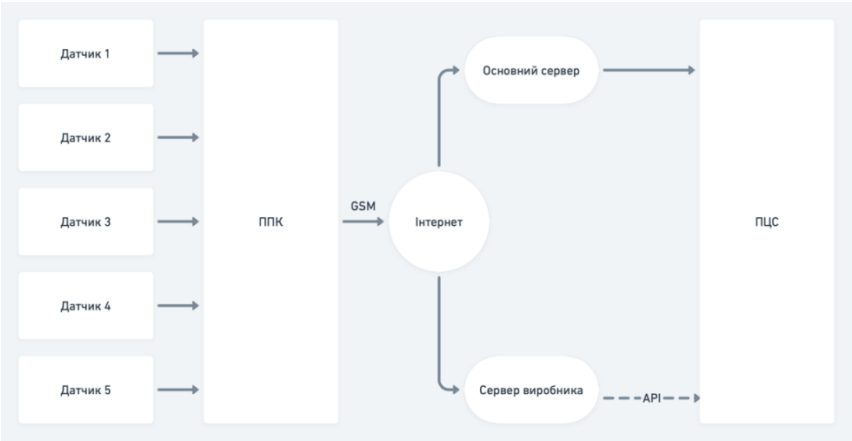


Рисунок 3.2 Використання API як резервний канал

Отримання того ж Api від виробника обладнання значно б покращило стійскість системи в цілому

Використання програмних рішень виробників, як резервний канал (по суті пряме використання серверних можливостей виробника, але тим самим можна уникнути вразливостей власного ПО і дозягаючи тим самим диверсифікації ризиків)

Зазвичай виробники, пишуть програми спеціально розроблені під використання, як альтернатуву ПЦН, які є на ринку в охоронних компаніях, але вони рідко набираають популярність тому, що зазвичай охоронні компанії використовують аппаратні рішення різних виробників, і тому використання велико кількості ПО під кожного виробника є неможливим. Але наявність такого програмного рішення значно покращує захищенність системи.

Ці програми, зазвичай, потребують невиликої потужності від апаратного засобу на якому їх запускають, але мають не менш різноманітний функціонал. Як такий тип каналу буде виглядаати на схемі – можна ознайомитись на рисунку 3.3

Важливим звісно є не тільки наявність, та правильне налаштування такого апаратно-програмного засобу (що не є зовсім складним), а написання процесів та навчання персоналу для роботи в екстренній ситуації.

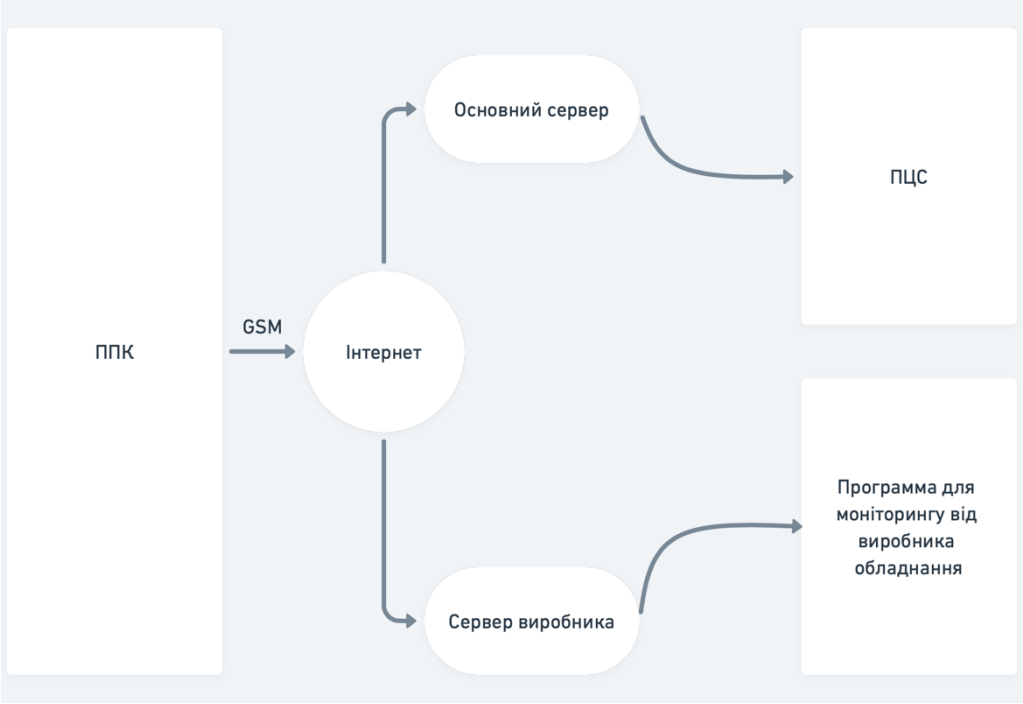


Рисунок 3.3

**Висноки за розділом 3**

В цьому розділі ми надали певні рекомендації, які можуть буди використані в розробці та побудові будь-якої ланки в створенні охоронної системи.
Основним наявним недоліком в сучасних охоронних системах є канали зв’язку, які використовуються в ПЦС та ППК.
Ми розлянули окремо рекомендації, які можемо надати для різних систем, та імплементувати та використати для створення дійсно надійної системи.

В першу чергу ми розлянули ППК, та які з наявних в сучаних системах типи рекомендується використувавути - це гібридні системи (тобто ті які здатні працювати з провідними та бездротовими датчиками)

А також рекомендується розглядати системи з мінімум трьома незалежними каналами зв’язку.

Також окремою рекомендацією хотілось би виділити ДВЧ передавачі. Завдяки яким ППК забезпечується ще одним каналом зв'язку з ПЦС. З модулем vhfBridge систему можна використовувати у містах з нестабільним інтернетом, горах, природно-заповідних зонах або пустельній місцевості.

З багатьох причин цей метод зв’язку є вкрай корисним як резервний канал, так як він єдиний не спирається на жодне інтернет підключення (Ethernet/Wi-Fi/GSM зв’язок). Особливо гостро це питання постає в період війни, коли жодний інтернет провайдер не може гарантувати стабільне підключення до мережі, не кажучи вже про мобільних операторів, з якими спостерігаються надзвичайні труднощі.

Також ми надали рекомендації для налаштування та використання кожного з трьох найпопулярніших каналів - Ethernet/Wi-Fi/GSM.

Також окремо для ПЦС було розроблені деякі рекомендації, які можуть бути використані охоронними компаніями для побудови дійсно якісного та безпечного комплексу ПЦС з багатьма резервними каналами зв’язку і що важливо – запропоновано використання ДВЧ частотних передавачів, як канали зв’язку який взагалі не залежить від мережі інтернет, що є його перевагою над всіма доступними раніше каналами зв’язку.

# ВИСНОВКИ

У своїй дипломній роботі я провів дослідження про актуальні типи та принципи роботи охоронних систем для розуміння того, які є основні недоліки та вразливості в сучасних ОС, так яык з швидким розвитком цієї галузі, і розвитку всіх технологій в цілому, за останні десятиліття данні системи сильно видозмінились, через що з’явилось багато вразливостей.

Після цього я провів детальний аналіз про способи створення актуальних та безпечних ОС, які недоліки найчастіше використовуються.

В цій роботі також були розглянуті основні методи, які використовуються в системах виробниками, або охоронними компаніями, для створення засобів захисту від загроз.Був проведений аналіз різних способів захисту від атак на основі різних систем та типів ОС.

Отримана інформація продемонструвала наявність великої кількості загроз, притаманних системам безпеки. Такі результати лише підтверджують той факт, що системи безпеки – це сфера, якій вкрай необхідна постійне спостереження та аналіз вразливостей, а також розвиток в сфері кібербезпеки, особливо врахочуючи чималий ріст ринку та розвиток цієї індустрії. Загалом питання безпеки ОС є надзвичайно важливим та ніколи не можна нехтувати ним: не зважаючи на те, чи ми говоримо про домашню сигналізацію чи охоронну систему банку.
Я розробив рекомендації, які можуть бути в нагоді як користувачам, так і охоронним компаніям/виробникам систем.

Таким чином, у результаті виконання даної роботи було досягнуто початкову мету та виконано усі необхідні для цього завдання.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке охоронна сигналізація периметру? [Електронний ресурс] // Klaster. – 2014. – Режим доступу до ресурсу: https://klaster.ua/ua/stati-i-obzory/chto-takoe-okhrannaja-signalizacija-perimetra/

2. Як працює охоронна сигналізація [Електронний ресурс] // Bezpeka Club. – 2020. – Режим доступу до ресурсу: https://bezpeka.club/yak-pratsyuye-ohoronna-sygnalizatsiya/

3. The history of the alarm system [Електронний ресурс] // Abus. – 2013. – Режим доступу до ресурсу: https://www.abus.com/eng/Guide/Break-in-protection/Alarm-systems/History-of-the-alarm-system

4. The Holmes Electric Protective Company [Електронний ресурс] //. – uv201. - 2019. – Режим доступу до ресурсу: http://uv201.com/Misc_Pages/holmes_history.htm

5. BS EN ISO 9001:2015 [Електронний ресурс] // European Standards . – 2019. – Режим доступу до ресурсу: https://www.en-standard.eu/bs-en-iso-9001-2015-quality-management-systems-requirements/

6. 24-hour Monitoring Services [Електронний ресурс] // Chubb. – 2019. – Режим доступу до ресурсу: https://www.chubbfiresecurity.com/en/sg/services/monitoring/

7. Graded vs Ungraded: What is a graded security alarm? [Електронний ресурс] // Boundary. – 2022. – Режим доступу до ресурсу: https://boundary.co.uk/blog/graded-vs-ungraded-alarms/

8. Sokullu R. Gts attack: An ieee 802.15. 4 mac layer attack in wireless sensor networks / R. Sokullu, I. Korkmaz, O. Dagdeviren. // International Journal On Advances in Internet Technology. – 2009. – №2. – С. 104–114.

9. How Does a Burglar Alarm Work? [Електронний ресурс] // Fireaction. – 2017. – Режим доступу до ресурсу: https://fireaction.co.uk/news/how-does-a-burglar-alarm-work/

10. Working Principle of Burglar Alarm [Електронний ресурс] // Studiousguy. – 2017. – Режим доступу до ресурсу: https://studiousguy.com/working-principle-burglar-alarm/

11. Управління GS модулем AVR [Електронний ресурс]. –Режим доступу: https://habr.com/ru/post/256349/ -Дата доступу: 20.01.2022.

12. Сигнализация на микроконтроллере [Електронний ресурс]. –Режим доступу: https://bezkz.su/publ/shemy/raznoe-na-mikrokontrollerah/300414-31-1-0-414.html-Дата доступу: 25.01.2019

13. Проектування мікропроцесорних систем: Проектування мікропроцесорних систем на базі AVR–мікроконтролерів: Периферійні модулі AVR-мікроконтролерів: Навчальний посібник для студентів напряму підготовки 6.050201 «Системна інженерія» кафедри Автоматики та управління у технічних системах / Укл.: А.О. Новацький–К: НТУУ „КПІ”.

14. Живлення охоронних систем [Електронний ресурс]. –Режим доступу: https://algoritm.org/arch/arch.php?id=53&a=1058- Дата доступу: 20.02.2022.

15. Комп’ютерна електроніка: Мікропроцесорні системи: Програмування мікропроцесорних систем: Навчальний посібник для студентів напряму підготовки 6.050201 «Системна інженерія» /Автор.: А.О. Новацький–К: НТУУ „КПІ”, 2014–307с.

16. Датчики “Алай”систем[Електронний ресурс]. –Режим доступу: http://alay.com.ua/ops/ohrannaya-signalizaciya/ Дата доступу: 20.03.2022.

17. Electronic Components Datasheet Search [Електронний ресурс] Режим доступуhttp://www.alldatasheet.com/view.jsp?Searchword=L78l00&gclid=EAIaIQobChMI7LG7meLy4gIVGpSyCh1JpAP0EAAYASAAEgJnpvD_BwE Дата доступу: 22.03.2022.

18. ATTiny 13 datasheet [Електронний ресурс] http://www.alldatasheet.com/view.jsp?Searchword=ATTINY13&sField=4Дата доступу: 22.03.2022.