Міністерство освіти і науки України

1. СХІДНОУКРАЇНСЬКий НАЦІОНАЛЬНий УНІВЕРСИТЕТ
2. імені ВОЛОДИМИРА ДАЛЯ
3. Факультет \_\_\_\_\_\_\_\_інформаційних технологій та електроніки\_\_\_\_\_\_\_
4. (повне найменування факультету)
5. Кафедра \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_електронних апаратів \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
6. (повна назва кафедри)
7. ПОЯСНЮВАЛЬНА ЗАПИСКА
8. до дипломного проекту (роботи)
9. освітньо-кваліфікаційного рівня \_\_\_\_\_\_\_\_\_\_магістр \_\_\_\_\_\_\_\_\_\_\_\_\_\_
10. (бакалавр, спеціаліст, магістр)
11. спеціальності \_\_\_\_172 Телекомунікації та радіотехніка \_\_\_\_\_\_\_\_\_\_\_
12. (шифр і назва спеціальності)
13. на тему
14. **Дослідження принципів побудови систем безпеки, що використовують GSM канали.**

|  |  |  |
| --- | --- | --- |
| Виконав: студент групи РЕА-19дм | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | А. Є. Козак  |
| Керівник | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | к.т.н., доц. О. М. Іванов |
| Завідувач кафедри | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | к.т.н., проф.Ю. Е. Паеранд |
| Рецензент | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | д.т.н., проф.В. М. Смолій |

1. Сєвєродонецьк – 2021

**СХІДНОУКРАІНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**імені ВОЛОДИМИРА ДАЛЯ**

Інститут, факультет, відділення **інформаційних технологій та електроніки**

Кафедра **електронних апаратів\_\_\_**

Освітньо-кваліфікаційний рівень \_ **магістр** \_

Напрям підготовки **172 Телекомунікації та радіотехніка**

**ЗАТВЕРДЖУЮ**

Завідувач кафедри ЕА

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_»\_\_\_\_\_\_2020 року

**З А В Д А Н Н Я**

**НА ДИПЛОМНИЙ ПРОЕКТ СТУДЕНТУ**

 **Козак Артем Євгенович**

1. **Тема проекту:** Дослідження принципів побудови систем безпеки, що використовують GSM канали.
2. **Керівник проекту:** к.т.н., доцент О.М. Іванов

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від 07.09.2020 р.

№ 128/15.14

1. **Строк подання студентом проекту \_\_**20. 12. 2020 р.**\_**
2. **Зміст розрахунково-пояснювальної записки** (перелік питань, які потрібно розробити):
	1. Вступ
	2. Літературний огляд
	3. Аналіз сучасного стану систем безпеки
	4. Дослідження систем безпеки, що використовують gsm канали
	5. Дослідження технічних характеристик систем безпеки, що використовують gsm канали
	6. Охорона праці
3. **Консультанти розділів проекту**

|  |  |  |
| --- | --- | --- |
| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата |
| Завдання видав | Завдання прийняв |
| Охорона праці | проф. Смолій В.М. |  |  |

6. Дата видачі завдання\_\_\_\_\_\_\_\_1. 10. 2020 року\_\_\_\_\_\_\_\_\_

**Календарний план**

|  |  |  |  |
| --- | --- | --- | --- |
| №з/п | Назва етапів дипломногоПроекту (роботи) | Строк виконанняетапів проекту(роботи) | Примітка |
| 1 | Вступ | 1.10.20 |  |
| 2 | Літературний огляд | 14.10.20 |  |
| 3 | Аналіз сучасного стану систем безпеки | 27.10.20 |  |
| 4 | Дослідження систем безпеки, що використовують gsm канали | 30.10.20 |  |
| 5 | Дослідження технічних характеристик систем безпеки, що використовують gsm канали | 2.11.20 |  |
| 6 | Охорона праці | 28.11.20 |  |
| 7 | Оформлення пояснювальної записки | 10.12.20 |  |

Студент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Козак А. Є.

Керівник проекту\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Іванов О. М.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| формат | зона | Поз. | Позначення | Найменування | Кіл. | Примітка |
|  |  |  |  |  |  |  |
|  |  |  |  | Текстові документи |  |  |
|  |  |  |  |  |  |  |
| А 4 |  | 1 | ДПМ 172.03 ПЗ | Пояснювальна записка | 1 |  |
|  |  |  |  |  |  |  |
|  |  |  |  | Графічні документи |  |  |
|  |  |  |  |  |  |  |
| А4 |  | 2 | ДПМ 172.03 ГЧ | Графічна частина | 27 |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | . |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |
|  |  |  |  |  | ДПМ 172.03. ВП |
|  |  |  |  |  |
| ЗМН | лист | № докум. | підпис | Дата |
| Розроб. |  Козак Полулященко ОлександМихайлович |  |  | Дослідження принципів побудови систем безпеки, що використовують GSM канали. | Літ. | лист | листів |
| Перевір. | Іванов  |  |  |  |  |  | 3 | 104 |
| Рецензент | Смолій |  |  | СНУ ім. В.Даля гр. РЭА-19дм |
| Н. контр |  |  |  |
| Затв. | Паеранд |  |  |

 **РЕФЕРАТ**

Изм.

Лист

№ докум.

Підпис

Дата

Лист

5

ДПМ 172.03 ПЗ

Разраб.

 Козак

Перевір.

 Іванов

Реценз.

Смолій

Н. Контр.

Утверд.

Паєранд

Дослідження принципів побудови систем безпеки, що використовують GSM канали.

Лит.

Листов

104

ВНУ гр. РЭА-19дм

Пояснювальна записка до дипломного проекту містить:

сторінок - 104 , рисунків –7 , таблиць –5 , джерел літератури - 22

**Об'єкт дослідження** – Системи безпеки, що використовують GSM канали.

**Мета роботи –** Дослідження принципів побудови систем безпеки, що використовують GSM канали. Розробка заходів з охорони праці та техніки безпеки при виробництві та експлуатації електронних приладів.

У даній роботі об'єктом дослідження є принципи побудови систем безпеки, що використовують GSM канали.

**СИСТЕМИ ЦЕНТРАЛІЗОВАНОГО СПОСТЕРЕЖЕННЯ. ІНТЕГРОВАНІ СИСТЕМИ БЕЗПЕКИ. РАДІОСИСТЕМИ ПЕРЕДАЧІ СПОВІЩЕНЬ. GSM- КАНАЛИ. ПУНКТ ЦЕНТРАЛІЗОВАНОЇ ОХОРОНИ**

 ЗМІСТ

Список умовних скорочень. …………………………………………………..7

Вступ…………………………………………………………………………….8

1.Літературний огляд ………………………………………………………….11

1.1. Основні поняття …………………………………………………………11

 1.2. Аналіз сучасного стану систем безпеки.………………………………..19

1.3. Використання бездротових каналів в системах охорони ……………....29

1.4. Огляд існуючих систем безпеки, що використовують gsm канали …....37

2. Дослідження систем безпеки, що використовують gsm канали …………50

2.1. Організація систем безпеки на основі gsm- каналів……………………..50

2.2. Дослідження принципів шифрування gsm каналу ………………………61

2.3. Функції gsm каналів, які використовуються системами безпеки………..67

2.4. Аналіз завадостійкості і перешкодозахищеності gsm каналу……………76

2.5. Дослідження швидкості передачі даних і пропускної здатності gsm каналу. …………………………………………………………………………………….80

3. Дослідження технічних характеристик систем безпеки, що використовують gsm канали ……………………………………………………………………….84

4. Охорона праці………………………………………………………………….89

4.1. Аналіз небезпечних і шкідливих факторів при виробництві……………...89

4.2. Заходи з охорони праці……………………………………………………..92

Висновки………………………………………………………………………..102

Література………………………………………………………………………103

 Список умовних скорочень

СЦС - системи централізованого спостереження

ІСБ - інтегровані системи безпеки;

РСПС – радіо системи передачі сповіщень

ПЦС - пункт централізованого спостереження;

ОПС – охоронна промислова система;

ПКП - приймально-контрольні прилади;

 МТП - мережі термінальних пристроїв;

УКХ –ультра - короткі радіохвилі.

 Вступ

 Існуючі охоронні комплекси в недавньому минулому проектувалися або як автономні, в цьому випадку якщо і передбачався контроль охоронюваних об'єктів, то з використанням складного і дорогого обладнання, або пов'язаний з використанням послуг оператора з контролю стану.

Подібні комплекси проектувалися і потім впроваджувалися окремо для кожного приміщення і потім об'єднувалися для довільної частини будівлі, в один досить складний і громіздкий комплекс. У будівлях встановлювалися системи тільки з тими можливостями і з тим ступенем складності, які були необхідні на поточний момент функціонування будівлі. Подальше розширення і модернізація таких охоронних комплексів було малоефективним через наступні фактори :

- Висока вартість впровадження подібного роду систем;

- Висока вартість експлуатації через необхідність тримати штат із супроводу подібних систем;

- Окрема підтримка всіх автономних систем;

- Висока вартість навчання персоналу, оскільки оператори повинні бути ознайомлені з кожною автономною системою.

Будь-який об'єкт має свої специфічні властивості, які визначають кінцевий вигляд інтегрованої системи безпеки. Тому проектування системи безпеки завжди жорстко прив'язане до кінцевого об'єкту, враховуючи всі його особливості: характеристики приміщень, інженерно-технічних систем, огороджувальних конструкцій, їх відповідності нормативно-технічної документації (СНІП, ГОСТ та інші), концептуальні вимоги забезпечення безпеки, оперативну обстановку в районі знаходження приміщення. Все це дозволяє досягти високого рівня безпеки.

Організація систем безпеки на основі GSM- каналів і передачі GPS координат якраз і є вирішенням даної проблеми. У проектований охоронний комплекс вже закладені кошти сучасних інформаційних технологій. У такій системі безпеки передбачена можливість отримання інформації в будь-якому місці іі будь в який час, як при наявності об'єднаної диспетчерської, так і в разі, коли диспетчерська відсутня зовсім, тобто система функціонує абсолютно автономно і незалежно. Крім отримання оптимальних рішень з точки зору якості і економічності системи безпеки реалізація подібної системи дозволяє значно спростити як проектування, так і монтаж інтегрованої системи. Для вже існуючих об'єктів, особливо там, де немає можливості прокладки кабельних ліній.

До основних переваг такої охоронної системи можна віднести:

• Доступність і відносно просту схему установки;

• Простоту управління і програмування;

• Контроль за системами життєзабезпечення будівлі

• Дистанційне керування виходами виконавчих пристроїв;

• Можливість прослуховування приміщення протягом певного часу при спрацьовуванні датчика (віддалено).

• Можливість функціонування при перебоях в електропостачанні;

• Відсутність жорсткої зв'язки між управлінням виконавчими пристроями і виникненням події;

• Можливість установки кнопки екстреного виклику служби охорони або міліції. За допомогою такої кнопки можна подати сигнал, перебуваючи в будь-якому місці будинку або неподалік від будинку.

 Основу централізованої охорони складають системи централізованого спостереження (СЦС). На початку свого розвитку найбільш широке застосування знайшли СЦС, що використовують в якості каналів зв'язку телефонні лінії. Це цілком зрозуміло. Устаткування таких систем порівняно дешево, а майже повсюдна телефонізація дозволяє підключати до них практично будь-які об'єкти. Спочатку на нашому ринку майже повністю були відсутні системи закордонного виробництва. Зарубіжні СЦС - це, як правило, інформаторні системи, які не вимагають для своєї роботи установки додаткового обладнання на АТС і передають тривожну інформацію шляхом прямого автодозвона на пульт. Істотним недоліком таких систем є відсутність контролю каналу зв'язку, що не дозволяє забезпечити надійну охорону об'єктів через простоту їх «обходу». Досить провести обрив телефонної лінії, і тривожна інформація буде загублена, а сам факт обриву не зафіксується на пульті. І саме тому одним з основних вимог позавідомчої охорони є обов'язкова наявність контролю каналу зв'язку, незважаючи на те, що система буде трохи дорожче і складніше. Хоча до сих пір навіть великі комерційні моніторингові компанії використовують інформаторні системи.

 Таким чином можна визначити наступні пріоритетні напрямки в створенні і розвитку СЦС:

1. Системи повинні мати модульну структуру з повним комплектом пристроїв, що дозволяє забезпечувати роботу по будь-яким наявним на сьогоднішній день (і навіть перспективним) каналам зв'язку, можливість стикування з уже існуючими системами, а також сполучення з різними типами апаратури, використовуваної для організації телефонного зв'язку ( нові електронні АТС, системи цифрового ущільнення, оптоволоконні канали зв'язку і т.п.). Всі ці можливості повинні бути реалізовані на єдиній програмно-апаратній платформі.

2. Протоколи обміну, використовувані для передачі тривожних і службових повідомлень, повинні бути захищені від несанкціонованого втручання в роботу системи за допомогою спеціальних засобів зняття та внесення неправдивої інформації в канали зв'язку.

3. Інформативність систем повинна забезпечувати рівень моніторингу стану об'єкта, максимально підвищує оперативність реагування груп затримання. Темою даної роботи є дослідження принципів побудови систем безпеки, що використовують GSM канали

 1. Літературний огляд.

 1.1. Загальні відомості.

 В даний час ринок послуг та обладнання охоронно-пожежної сигналізації стрімко зростає. Однак до недавнього часу основним недоліком систем охоронної та пожежної сигналізації (ОПС) було використання дротяних телефонних ліній. До основних недоліків даних систем можна віднести нестійку роботу міських телефонних ліній, низьку фізичну захищеність, відсутність можливості охорони не телефонізованих об'єктів (дачі, котеджі і т. Д.). Тому в якості надійної альтернативи «провідних охоронних систем» з'явився новий напрям або «радіоканальні охоронні системи».

Переваги радіоканальних охоронних систем очевидні:

- відсутність залежності від телефонної лінії і якості роботи мережі;

 - простота монтажу;

 - можливість охорони будь-якого об'єкта (в межах зони дії радіоканальної мережі).

 - універсальність - з простих елементів можна побудувати скільки завгодно складну систему: висока швидкість монтажу і запуску в експлуатацію, можливість оперативного зміни конфігурації, мобільність охоронного пульта, можливість співіснування кількох пультів. Немає принципових обмежень для підключення в разі потреби до існуючої системи охорони. Незважаючи на очевидну ефективність централізованої охорони, при впровадженні та експлуатації СЦС виникають певні проблеми, на яких хотілося б зупинитися нижче.

 Перша з них пов'язана з підвищенням «професійного» рівня кримінального контингенту. Останнім часом з'явилися випадки «кваліфікованих» крадіжок, скоєних шляхом активного, тобто із застосуванням спеціальних технічних засобів, втручання в роботу обладнання та каналів зв'язку СЦС. І якщо зараз відомі лише окремі подібні випадки, то в самий найближчий час це може стати масовим явищем. Єдиний шлях вирішення даної проблеми, а це, безсумнівно, одна з найважливіших проблем самого найближчого майбутнього, - застосування сучасних методів імітостойкості апаратури і криптозахисту каналів зв'язку, які забезпечують стійкість системи до несанкціонованого втручання в її роботу.

 Друга проблема - це організація охорони так званих «великих об'єктів». Це об'єкти кредитно-фінансової сфери, особливої ​​важливості, підвищеної небезпеки, життєзабезпечення і їм подібні.

 В даний час найбільш перспективним і загальновизнаним шляхом організації їх захисту є застосування інтегрованих систем безпеки (ІСБ). ІСБ в системах централізованої охорони являє собою об'єктове обладнання, проте кількість інформації, яке необхідно передавати на пульт і приймати з боку пульта, в цьому випадку значно зростає. Особливо це пов'язано з застосуванням у складі ІСБ телевізійних систем, які в даний час широко застосовуються для підвищення безпеки різних об'єктів.

 Відповідно до цього, актуальним завданням є створення пари високоінформативного обладнання ІСБ з обладнанням СЦС. Домогтися максимальної ефективності функціонування ІСБ і систем централізованої охорони в цілому можливо тільки підвищенням їх інформативності, яке дозволяє оптимізувати дії груп затримання за рахунок постійного моніторингу поведінки злочинця на об'єкті або розвитку інших негативних ситуацій (наприклад, пожежі). Особливо це стосується критично важливих об'єктів, де оперативність прийняття рішень, грамотний розподіл сил і засобів відіграють першорядну роль.

 Третя і, мабуть, найсерйозніша проблема, що стосується провідних СЦС, а вони на сьогоднішній день, як вже було зазначено, займають домінуюче становище, обумовлене технічною політикою компаній, що надають послуги телефонного зв'язку. Будучи в якійсь мірі монополістом в своїй галузі, необґрунтовано підвищують ціни на оренду телефонних ліній і площ на АТС, заздалегідь не інформують охоронні структури про майбутні реконструкціях, заміні і параметрах нового обладнання на телефонних станціях.

 Єдиний шлях вирішення даної проблеми - це застосування альтернативних каналів зв'язку для організації централізованої охорони. За своїм принципом їх можна розділити на дві групи: провідні і бездротові. До недавнього часу єдиним з «альтернативних» застосовувався лише виділений радіоканал (РСПІ). Останнім часом, крім традиційного радіоканалу, все активніше починають використовуватися інші альтернативні канали (GSM, Інтернет та ін.). Вибір застосовуваного каналу зв'язку залежить від багатьох факторів. Розглянемо їх трохи докладніше.

 Мережа стандарту GSM зараз має найширшу зону покриття, що робить її дуже привабливою для організації централізованої охорони. З огляду на, що основна мета її створення - це передача мовних повідомлень, основний канал, що має певні пріоритети - це голосовий канал. Крім голосового каналу, в GSM-мережі існує цифровий канал даних, канал GPRS (EDGE) і з недавнього часу високошвидкісний канал 3G. При використанні кожного із зазначених каналів для цілей охорони необхідно розуміти їх особливо

 У голосовому каналі існує явище «хендовер». Так називається будь-перемикання на інший канал або тайм-слот однієї і тієї ж стільники. Таке перемикання відбувається при різкому збільшенні навантаження на стільникову мережу, наприклад, після футбольного матчу або при приземленні літака. При такому перемиканні відбувається зміна спектру сигналу, що є допустимим для передачі мови і неприйнятно для передачі цифрової інформації. Але ж для цілей охорони по голосовому каналу буде передаватися саме «цифра». Тобто при виникненні такого явища канал зв'язку стає вкрай нестійким. Для передачі цифрової інформації в мережах GSM існує спеціальний канал цифрових даних. Швидкість передачі невелика, але достатня для передачі повідомлень в невеликому обсязі, схожому по інформативності з Contact-ID. Повідомлення передаються без спотворень. Але передача інформації через цифровий канал даних буде доступна лише, якщо мережа не буде завантажена, оскільки в існуючих GSM-мережах загального користування пріоритет віддається голосовому каналу. Ця проблема частково вирішується шляхом використання каналу GPRS (EDGE). У цьому випадку застосовується протокол TCP / IP. Оператори пропонують спеціальні тарифи, при використанні яких канал буде доступний незалежно від завантаженості мережі. Але для використання GPRS рівень сигналу GSM повинен бути стабільно високим. Також на якість і швидкість цифрової передачі впливають «індустріальні перешкоди», які часто присутні в місті. Використання 3G схоже з GPRS, але значно підвищена інформативність. Однак покриття мереж 3G поки невелика, а обладнання помітно дорожче. Але найголовнішою проблемою використання GSM-каналів є досить проста можливість вимкнення (за допомогою так званих «глушилок»), а здійснювати надійний контроль каналу, наприклад, за допомогою спеціально призначених для корпоративних клієнтів віртуальних корпоративних мереж - досить дорого.

 Інша приваблива мережу, яка має загальне поширення - це Інтернет. Сьогодні отримати доступ до мережі можливо багатьма способами. При цьому застосовуються як провідні, так і сучасні бездротові технології. Але тут виникає потенційна небезпека несанкціонованого доступу до даних і внесення комп'ютерних вірусів. Крім того, дослідження показали, що багато разів упродовж доби виникають зникнення зв'язку на час від десятків секунд до декількох хвилин. Причиною цього є, як правило, перевантаження сервера провайдера, яка може бути викликана тривалою інформаційної завантаженістю одного з каналів в мережі, проведенням «хакерської» атаки і рядом інших причин. Причому вплинути на цей процес практично неможливо. Так влаштована апаратура цифрових каналів.

 Для того щоб уникнути негативних наслідків використання відкритих мереж загального користування (GSM, Інтернет), необхідно використовувати їх із застосуванням закритих виділених каналів або створювати свої незалежні мережі. В умовах міської забудови для цього підходить сучасний стандарт бездротового зв'язку WiMax. На сьогоднішній день вже розгорнуті комерційні мережі. Вони створені для доступу до Інтернету, цифрового телебачення та IP-телефонії. У майбутньому можливе їх використання для централізованої охорони, оскільки ця технологія дозволяє виділити незалежний закритий канал всередині розгорнутої мережі загального користування. Протокол, який використовується в WiMax, дозволяє надійно здійснювати контроль каналу без додаткових витрат, на відміну від GSM, а канал передачі даних має високу пропускну здатність, що особливо важливо для організації зв'язку з об'єктами, де необхідна велика інформативність. Вартість обладнання для доступу до мережі вже зараз можна порівняти з вартістю GSM-модему, що не створює додаткових перешкод для його впровадження. Насправді використовувати сучасний стандарт бездротового доступу для організації охорони можна вже і сьогодні.

 Однак, незважаючи на появу масових технологій бездротового доступу, ще тривалий час будуть зберігати своє значення як спеціалізований клас обладнання радіосистеми передачі сповіщень (РСПІ). В основі цього лежать як економічні фактори, так і прагнення більшості постачальників послуг до створення власної, незалежної від зовнішніх обставин, мережі передачі даних.

 Розглядаючи тенденції розвитку РСПІ, не можна не відзначити поступовий перехід від односторонніх способів обміну інформацією (від об'єктового обладнання до пультового) до двосторонніх.

 Такий перехід обумовлений такими факторами:

■ появою порівняно дешевої елементної бази, що серійно випускаються мікросхеми з функціями приймально-передавального радіотракта;

■ необхідністю економного ставлення до використання частотних ресурсів (при організації дисципліни опитування завжди можна збільшити кількість абонентів, що обслуговуються, але не за її відсутності);

■ можливістю надання спеціальних і сервісних функцій, що реалізуються тільки при можливості діалогу між центральним обладнанням і обладнанням, встановленим на об'єкті.

 Крім вищевказаних переваг, перехід до двостороннього способу обміну інформацією дозволив значно підвищити інформативність систем. Якщо раніше кількість видів інформації було досить жорстко обмежена (як правило, «Взято під охорону», «Знято з охорони», номери і типи порушених / відновлених шлейфів сигналізації, інформація про стан електроживлення і т.п.), то тепер ці обмеження пов'язані тільки з межами фантазії розробника. На жаль, фантазія більшості розробників не пішла далі старого доброго формату «Contact ID».

 З іншого боку, різке збільшення інформативності спілкування між об'єктовим і пультовим обладнанням в радіоканальних системах привело до виникнення ще однієї цікавої тенденції. А саме, до інтеграції з об'єктовими підсистемами інших виробників. Продаючи своє радіоканальне обладнання, виробник зацікавлений в тому, щоб його обладнання дозволило вирішити найбільшу кількість завдань, що виникають в реальному житті. Найбільш коротким шляхом до такої універсалізації є забезпечення можливості підключення максимальної кількості підсистем «нижнього» рівня зі збереженням їх повної інформативності. Наприклад, виробник РСПІ не може якісно реалізувати підсистему збору інформації від бездротових сповіщувачів або біометричну систему контролю доступу. Це краще вміють інші. Але він може домовитися про сполученні протоколів обміну інформацією. І в цьому випадку обидва партнери отримують взаємну вигоду. В цілому такі зміни носять позитивний характер. Оскільки кінцевий споживач залишається тільки у виграші, отримуючи поліпшені сервісні функції за ту ж ціну. Найбільш актуальними проблемами для вдосконалення РСПІ є два, на перший погляд, несумісні завдання. Зменшення використовуваної смуги робочих частот і підвищення швидкості обміну інформацією в радіоканалі. Використання смуг робочих частот шириною 25 кГц вже зараз стає анахронізмом. А в подальшому, при посиленні контролю над користуванням радіочастотного спектру, стане економічно недоцільним. З іншого боку, безперервний розвиток об'єктових підсистем, в тому числі систем охоронного телебачення, постійно підвищує вимоги до пропускної здатності каналу зв'язку між об'єктової та пультової частиною. Це протиріччя залишає широкий простір для творчості.

 В даний час кількість приватних охоронних підприємств і моніторингових компаній тільки зростає, що тягне все більшу конкуренцію між ними. В умовах відсутності єдиної технічної політики в області організації централізованої охорони, яка визначає вимоги по надійності застосовуваних СЦС, деякі компанії йдуть по шляху зменшення витрат на шкоду надійності. Це призводить до зниження якості послуг, що надаються, тобто до загального зниження рівня безпеки та захищеності. В останні роки грань між містом і областю поступово стирається: одні переїжджають жити подалі від галасливого мегаполісу, інші проводять за містом більшу частину свого часу, і все більше людей хочуть захистити не лише свої квартири, але і нерухомість за межами міста. В таких умовах більшість моніторингових компаній використовують, як правило, канали стільникового зв'язку GSM. А, як говорилося вище, здійснення контролю стільникового каналу - річ досить витратна. На пульті НЕ буде інформації про те, що система вимкнена, зламалася або була навмисне виведена з ладу до 12 годин, а заявка технічній службі надійде лише після 72 годин «мовчання» системи. Про яку надійність такої організації охорони можна говорити?

 Таким чином, можна визначити наступні пріоритетні напрямки в створенні і розвитку СЦС:

 1. Системи повинні мати модульну структуру з повним комплектом пристроїв, що дозволяє забезпечувати роботу по будь-яким наявним на сьогоднішній день (і навіть перспективним) каналам зв'язку, можливість стикування з уже існуючими системами, а також сполучення з різними типами апаратури, використовуваної для організації телефонного зв'язку ( нові електронні АТС, системи цифрового ущільнення, оптоволоконні канали зв'язку і т.п.). Всі ці можливості повинні бути реалізовані на єдиній програмно-апаратній платформі.

 2. Протоколи обміну, використовувані для передачі тривожних і службових повідомлень, повинні бути захищені від несанкціонованого втручання в роботу системи за допомогою спеціальних засобів зняття та внесення неправдивої інформації в канали зв'язку.

 3. Інформативність систем повинна забезпечувати рівень моніторингу стану об'єкта, максимально підвищує оперативність реагування груп затримання.

 Спочатку бездротові системи не отримали широкого поширення через низьку надійності (дротяний зв'язок в цьому плані ще років п'ять назад була надійніше). Але в даний час з'явився широкий спектр різних додатковими пристроїв, активно використовуються нові покоління бездротових систем зв'язку. Повсюдне використання стільникових систем зв'язку не могло не позначитися на системах охорони. Можливості, що надаються операторами стільникового зв'язку все активніше використовуються в системах охорони. Також можна бачити, що GSM канали зв'язку ще не вичерпали ліміт свого розвитку. На сьогоднішній день бездротові охоронні системи на базі GSM набули широкого поширення завдяки їх відносно невисокій вартості і простоті установки і експлуатації. Мережа стандарту GSM-900/1800 забезпечує кращу якість зв'язку і вже розгорнута в більшості міст України і країн СНД.

 Системи, що використовують GSM-зв'язок, дозволяють здійснити охорону будь-яких об'єктів, в тому числі і не телефонізованих. Використання GSM позбавляє від необхідності розгортати свою мережу ретрансляторів - використовуються ретранслятори GSM-операторів. Внаслідок цього можна брати під охорону об'єкт всюди, де впевнено працює мережа GSM-оператора. І, звичайно, дуже перспективним видається використання нових протоколів і мереж 3G, спеціально призначених для корпоративних клієнтів - віртуальні корпоративні мережі передачі даних з імітостійкістю і захистом інформації. Однак суттєвим недоліком подібних систем є низька перешкодозахищеність. Не секрет, що GSM-канал легко придушити, «GSM глушилки» знаходяться сьогодні у вільному продажі, та й робота мережі GSM не завжди відрізняється високою стабільністю і може відмовити в самий невідповідний момент. Хоча останні розробки дозволяють повністю контролювати GSM-канал, оперативно змінювати частоти, що помітно підвищує перешкодозахищеність Оптимально використовувати GSM-канал в якості дублюючого або додаткового до дротових або іншим радіоканальних систем. Величезний плюс GSM-систем - можливість самим клієнтом контролювати стан об'єкта і управляти його охороною.

 1.2. Аналіз сучасного стану систем безпеки.

 Сьогодні у світовій практиці охоронних послуг визначилася стійка тенденція на посилення ролі технічних засобів. Тенденція ця не випадкова: численні дослідження в області особистої і майнової безпеки показали, що широке використання технічних засобів дозволяє виключити або звести до мінімуму негативний вплив самої ненадійної ланки в системі охорони - людини, якій притаманні стомлюваність, неуважність, недбалість і т. п. При цьому, організація охорони з допомогою технічних засобів обходиться споживачеві значно дешевше, а надійність її вище. Більш ніж 50-річний досвід роботи позавідомчої охорони в цій області показав, що найбільш ефективним і економічно вигідним видом є централізована охорона. Суть її в тому, що інформація від технічних засобів, встановлених на територіально розосереджених об'єктах, надходить безпосередньо на центральний пульт, де в автоматизованому режимі проводиться її аналіз, узагальнення та видача заявки на реагування, в залежності від ситуації, міліцейському поряд або технічній службі.

 Технічну основу централізованої охорони складають системи централізованого спостереження (СЦС).

 Найбільш широке застосування, як у нас, так і за кордоном знайшли СЦС, що використовують в якості каналів зв'язку телефонні лінії. Це цілком зрозуміло. Устаткування таких систем порівняно дешево, а майже повсюдна телефонізація дозволяє підключати до них практично будь-які об'єкти. З огляду на, що практично з самого початку утворення позавідомча охорона України в рамках однієї структури забезпечувала одночасне вирішення трьох основних функцій: технічної (охорона за допомогою технічних засобів), поліцейської (реагування нарядами поліції) і страхової (відшкодування матеріального збитку), саме до технічної складової завжди пред'являлися підвищені вимоги по надійності з метою зниження витрат по двох інших.

 В середині 90-х років при створенні СЦС основна увага приділялася таким аспектам, як:

- автоматизація, яка дозволяє до мінімуму спростити процеси здачі / взяття об'єктів під охорону, скоротити черговий персонал пультів централізованої охорони; істотно скоротити кількість помилкових тривог через неправильні дій господарчих органів;

- контроль каналу зв'язку, що забезпечує високу достовірність передачі і виключає втрату тривожної інформації;

- розробка широкої гами об'єктових пристроїв з різними функціональними і сервісними можливостями, що дозволяють задовольнити потреби самих широких верств населення.

 З урахуванням цих вимог були розроблені і впроваджені такі системи, як «Юпітер», «Приплив-А», «Фобос-А», «Фобос-3» та інші.

 З точки зору організації захисту об'єктів від несанкціонованого проникнення (як по обладнанню технічними засобами охорони, так і з тактики дій чергових служб) всі перераховані СЦС не мають яких-небудь істотних відмінностей, проте, кожна з них має свої достоїнства і недоліками, які визначають і обмежують область їх застосування.

 Однак головним недоліком зазначених систем є різнорідність технічних і конструктивних рішень, а також закрита архітектура побудови, що не дозволяє провести їх об'єднання в єдиний універсальний комплекс технічних засобів централізованої охорони в межах одного ПЦО. Це, в кінцевому, підсумку призводить до виникнення певних проблем для всіх структур позавідомчої охорони у впровадженні, експлуатації, обслуговуванні та ремонті різнорідних технічних засобів, в проведенні єдиної технічної політики, забезпеченні належного рівня якості і надійності обладнання, а, отже, до додаткових фінансових витрат і збільшення тарифів на охоронні послуги.

 Саме тому, найбільш актуальною залишається на сьогоднішній день проблема впорядкування парку експлуатації систем централізованого спостереження, його поновлення, заміни застарілого обладнання сучасним, більш надійним.

 Тому з метою подальшого розвитку та вдосконалення централізованої охорони до нових розробок останнім часом висуваються додаткові вимоги:

- імітостійкість і криптозахист, що забезпечують стійкість системи до несанкціонованого «обходу» і обумовлені появою «кваліфікованих» крадіжок;

- висока інформативність, що забезпечує поділ сигналів про проникнення і пожежі, аварії або зміні параметрів лінії зв'язку і т. д .;

- можливість сполучення системи з оптоволоконними каналами зв'язку, обумовлена ​​впровадженням підприємствами зв'язку нових цифрових технологій передачі інформації;

- уніфікація створюваних технічних засобів, тобто можливість об'єднання різних пристроїв в єдиний програмно-апаратний комплекс централізованої охорони.

Пріоритетним завданням технічної політики в галузі розвитку централізованої охорони є розробка відсутніх на сьогоднішній день єдиних вимог на системи централізованого спостереження, що в умовах різноманіття існуючих і тих,що з'являються знову підприємств-розробників і виробників засобів охоронно-пожежної сигналізації дозволить уніфікувати стики систем передачі сповіщень, як тих, що розробляються , так і тих, що вже знаходяться в експлуатації.

 В останні роки особлива увага приділялася створенню і розвитку радіосистем передачі сповіщень (РСПС). Впровадження охоронних систем, що використовують радіочастотні канали зв'язку, дозволяє:

- розширити сферу діяльності підрозділів позавідомчої охорони шляхом організації охорони об'єктів, що не мають лінії телефонного зв'язку;

- підвищити надійність систем охорони особливо важливих об'єктів за рахунок дублювання телефонних каналів зв'язку;

- забезпечити при необхідності термінову установку устаткування на об'єкті, який потребує охорони.

 Діяльність НДЦ «Охорона» в даній області була спрямована на здешевлення обладнання радіосистем, з метою підвищення його доступності для населення.

У той же час якість систем, як щодо споживчих властивостей, так і щодо надійності і захищеності переданої інформації, має постійно підвищуватися.

З цією метою перспективним напрямком є ​​створення радіосистеми ближнього радіусу дії зі зниженою вартістю об'єктового обладнання і поліпшеними тактико-технічними, вартісними і експлуатаційними параметрами, що дозволяє організувати охорону таких об'єктів як гаражні та дачні кооперативи, садівничі товариства і т. п.

 Переваги радіо канальних охоронних систем очевидні:

- відсутність залежності від телефонної лінії і якості роботи мережі;

- простота монтажу;

- можливість охорони будь-якого об'єкта (в межах зони дії радіо канальної мережі).

 На сьогоднішній день все бездротові системи можна розділити на чотири групи:

- GSM системи;

- радіо канальні системи малого радіусу дії;

- радіо канальні системи великого радіусу дії;

- супутникові системи.

 GSM-системи набули широкого поширення на початку XXI століття після бурхливого розвитку мобільного зв'язку. Спочатку в якості каналотворного обладнання використовувалися мобільні телефони, які підключалися до охоронних панелям через інтерфейс RS-232 і управлялися AT-командами. Дане рішення було дуже ненадійним, так як телефони могли зависнути або просто відключитися, крім того, умови експлуатації мобільних телефонів не передбачали роботу в сирих і неопалюваних приміщеннях, що істотно обмежувало область їх застосування. Сьогодні, виробники обладнання мобільного зв'язку випускають спеціалізовані GSM-модеми (M2M-рішення) для побудови на їх основі бездротових систем безпеки. Дане рішення істотно підвищило надійність роботи системи, а також надало розробникам систем безпеки додаткові можливості по роботі з сервісами GSM (рис.1.1). Як спосіб передачі інформації в GSM-системах використовуються SMS-повідомлення, модемне з'єднання (CSD), передача тонових посилок (режим DTMF) і режим пакетної передачі повідомлень GPRS. Поява режиму GPRS дозволила істотно знизити витрати на експлуатацію систем радіо охоронних. На сьогоднішній день бездротові охоронні системи на базі GSM набули широкого поширення завдяки їх відносно невисокій вартості і простоті установки і експлуатації. Однак суттєвим недоліком подібних систем є низька перешкодозахищеність. Не секрет, що GSM-канал легко придушити, «GSM глушилки» знаходяться сьогодні у вільному продажі, та й робота мережі GSM не завжди відрізняється високою стабільністю і може відмовити в самий невідповідний момент. Зазначені недоліки обмежують застосування обладнання подібного класу при побудові систем безпеки. Дані системи більшою мірою застосовуються в якості резервних (додаткових) каналів зв'язку або для побудови систем моніторингу віддалених об'єктів для збору телеметричної інформації.



Рис.1.1. Схема передачі інформації в GSM охоронної системі при використанні функції SMS.

 GSM охоронна система може включати в себе один або де- кілька GSM контролерів серії TSS-705, а також засоби контролю і управління цими GSM контролерами - мобільні телефони та (або) комп'ютери.

GSM контролери встановлюються на віддалених об'єктах. До кожного з них можна підключати:

- Різні дискретні і резистивні датчики. Наприклад, контактні датчики, геркони, терморезистори для контролю температури, датчики охоронної та пожежної сигналізації і т. п .;

- Відеокамери (до 3 кольорових або чорно-білих відеокамер (PAL або NTSC) на один контролер);

- Мікрофон і звуковий динамік;

- Виконавчі пристрої (контролер має 3 реле для управління такими пристроями);

- Кнопки для установки датчиків на охорону безпосередньо на об'єкті;

- Кнопки та (або) зчитувач коду різних ідентифікаторів (карт, брелоків) для зняття датчиків з охорони;

Приклади систем: РСПС "Риф Стрінг-202", "Стрілець", "Дельта".

До радіо канальних систем малого радіусу дії відносяться бездротові системи, що працюють в частотному діапазоні (433 МГц і 2,4 ГГц) з малою вихідною потужністю (10 мВт і 100 мВт відповідно). В основному дані системи застосовуються для організації локального бездротового зв'язку на території великих об'єктів. Радіус дії таких систем становить зазвичай від кількох сотень метрів до кількох кілометрів в залежності від умов поширення радіосигналу. При цьому пункт централізованого спостереження (ПЦС) зазвичай розташовується на цьому ж об'єкті, або організовується спеціальний виділений канал зв'язку для передачі інформації на віддалений ПЦС. В даний час дані системи набули широкого поширення завдяки їх відносно низькій вартості і простоті монтажу. На сьогоднішній день все більше і більше популярні приймачі стандарту 2,4 ГГц, такі як ZigBee, NanoNet і ін. Дані передавачі випускаються в одно кристальному виконанні з підтримкою стека високорівневих протоколів, що, безумовно, спрощує розробку систем бездротового зв'язку на їх основі і дає розробникам широкі можливості по реалізації алгоритмів обміну даними. Недоліком даних систем є їх низька перешкодозахищеність і малий радіус дії.

 До радіо канальних систем великого радіусу дії. відносяться системи, що мають виділений радіоканал і забезпечують радіус дії 20-100 км в умовах міської забудови. До складу даних систем входять абонентське обладнання, ретранслятори (базові станції) і пульт централізованого спостереження. Здебільшого системи даного класу використовують частотний діапазон 146-174 МГц і вихідну потужність 1-10 Вт. З точки зору організації радіо інтерфейсу системи можна розбити на дві групи. Системи, що використовують стандартні УКХ-радіо інтерфейси. Такі системи, як правило, використовують частотну маніпуляцію і ширину каналу 12,5 або 25 кГц. Недоліком таких систем є низька пропускна здатність і невисока перешкодозахищеність, так як сигнал з смугою 12,5 кГц легко придушити. Системи, що використовують спеціалізовані радіо інтерфейси використовують радіо інтерфейси, адаптовані під вирішення завдань радіо охоронних і забезпечують захист інформації і високу перешкодозахищеність каналу зв'язку. Прикладом такої системи є радіо канальні система АРКАН, що використовує для передачі вузько смугові сигнали і алгоритм «стрибаючих частот». Перебудова частоти відбувається за випадковим законом в широкій смузі (300-500 кГц). Дане рішення забезпечує високу перешкодозахищеність і високу ємність системи. До недоліків радіо канальних систем великого радіусу дії можна віднести високу вартість інсталяції мережі, однак при великій кількості абонентів ці витрати окупності. Дані системи широко застосовуються в середніх і великих містах на ПЦС з абонентською базою понад 2000-3000 абонентів.

 Супутникові системи використовують в якості каналів зв'язку супутниковий зв'язок ( «Глобалстар», «Інмарсат», «Турайя»). Подібні системи застосуються для контролю / охорони віддалених об'єктів, в місцях, де відсутній мобільний і дротяний зв'язок. Головним недоліком цих систем є висока вартість як абонентського обладнання, так і витрат на експлуатацію. З іншого боку, для вирішення завдань охорони віддалених одиночних об'єктів дані системи не мають іншої альтернативи. З точки зору питань сполучення ОПС і каналоутворюючого обладнання існує три рішення: ОПС з вбудованим радіо канальним обладнанням .Дане рішення просте і недороге, в одному корпусі ви отримуєте і охоронну панель з джерелом безперебійного живлення, і радіоканал. Недоліком даного рішення є невелика кількість охоронюваних зон, як правило, їх не більше 4-8. Але для невеликих об'єктів це цілком прийнятне і дуже економічне рішення.

 ОПС з зовнішнім радіо канальним обладнанням, що підключається через спеціалізований інтерфейс. Системи даного типу зазвичай пропонують виробники, які мають широку лінійку систем ОПС і різні типи канало утворюючого обладнання. Тому користувач може в залежності від конкретного завдання визначити для себе склад проектованої системи ОПС і зібрати «конструктор» з необхідних компонентів. Як правило, дані системи використовують шинні інтерфейси зв'язку між вузлами (наприклад, RS-485). Перевага даного підходу полягає в гнучкості проектування ОПС. Залежно від завдання ви можете вибирати контрольну панель з необхідною кількістю охоронних зон, використовувати радіоканал або проводове мовлення, при цьому все обладнання буде уніфіковано, мати єдину логіку роботи і єдині протоколи обміни. Недоліком даного рішення є те, що ви не зможете використовувати обладнання різних виробників, а це не завжди зручно, наприклад, у разі якщо ви збираєтеся використовувати системи ОПС одного виробника і радіоканал іншого.

 ОПС з зовнішнім радіо канальним обладнанням, що підключається через стандартний інтерфейс. Даний підхід вирішує проблему, описану вище. Використовуючи стандартний інтерфейс, можна використовувати обладнання різних виробників. Однак на сьогоднішній день виробники обладнання не прагнуть розробити єдиний стандарт, навпаки - використовують свої закриті протоколи. Єдиним відкритим стандартом сьогодні є інтерфейс Contact ID, розроблений компанією ADEMCO і призначений для передачі повідомлень по телефонних лініях в режимі тонових посилок DTMF. Більшість контрольних панелей мають даний інтерфейс. Тому єдиним рішенням для виробників канало утворюючого обладнання для охоронних систем було реалізувати всередині своїх пристроїв декодер ContactID. Дані рішення сьогодні широко застосовуються і в GSM-модеми, і радіоканальних системах. Користувач, в свою чергу, може вибирати, який канал зв'язку використовувати: провідний або бездротовий, при цьому устаткування ОПС перемонтувати і перенастроювати не потрібно, просто вихід ContactID підключається або до телефонної лінії, або на вхід радіопередавача.

 Однією з бездротових технологій,що найбільш швидко розвиваються, є ZigBee, яка спочатку розроблялася як низкошвидкісний канал зв'язку для об'єднання в мережу різних датчиків. Стосовно до безпеки це можуть бути датчики охоронної та пожежної сигналізації.

 Цілком можливо, незабаром ZigBee потіснить багато з існуючих сьогодні радіо канальних ОПС. Адже майже всі вони розроблені поза будь-якими стандартами. У кожного виробника - свої протоколи обміну, і замінити наявні на об'єкті бездротові датчики на обладнання іншого виробника неможливо. Якщо стандарт ZigBee набуде поширення, що цілком ймовірно, то замовник отримає можливість використовувати в системах ОПС практично будь-які датчики на вибір. Тим більше що стандартні профілі (специфікації наборів команд і протоколів обміну) для конкретних додатків в області автоматизації будівель і систем безпеки розроблені, опубліковані, і все це разом узяте гарантує сумісність обладнання різних виробників. Цей стандарт, не побоюся повторитися, хороший для з'єднання центрального вузла з периферією, яка розміщується територіально розподілена, причому за рахунок включення в систему ретрансляторів територія покриття може бути вельми великою. Теоретично можна використовувати ZigBee і в СКУД. Але цей канал має невелику швидкість передачі даних і невелику дальність. Погодьтеся, нераціонально будувати довгий ланцюжок ретрансляторів заради з'єднання контролера з комп'ютером. Є багато більш простих, а головне, дешевих і надійних способів.

Можна сказати, що всі перераховані технології на сьогоднішній день активно розвиваються і широко застосовуються для вирішення завдань охорони стаціонарних об'єктів. Вибір тієї чи іншої бездротової системи визначається в залежності від типу об'єктів, їх кількості, вимог до надійності доставки повідомлень і віддаленості об'єктів. У деяких випадках для підвищення надійності використовується резервування каналів зв'язку. Можна сказати, що майбутнє за бездротовими технологіями і скоро вони повністю витіснять з ринку провідні охоронні системи.

 1.3. Використання бездротових каналів в системах охорони

 Системи відеонагляду.

Першими в цій галузі з'явилися електронні пристрої, здатні віддавати лише текстові SMS-повідомлення з об'єкту, що охороняється. Таке пристрій складався з електричного блоку, до якого можна було підключити 1-4 зовнішніх датчика або шлейф охоронної сигналізації і звичайного мобільного телефону. Пристрій можна було встановити на будь-якому об'єкті, що має стійкий прийом GSM-мережі. Принцип роботи пристрою заснований на сповіщенні користувача за допомогою текстового SMS-повідомлення, яке передавалося на мобільний телефон користувача через GSM-канал в разі спрацювання охоронного датчика або порушення цілісності шлейфу охоронної сигналізації. Подібні пристрої спішно завоювали популярність серед власників невеликих заміських будинків і котеджів невисокою ціною і простотою установки. У відповідь власник подібного пристрою при отриманні SMS-повідомлення нескладно телефонував на мобільний телефон сусіда або місцевого сторожа, той, що в свою чергу, йшов до дому і з'ясовував причини спрацювання. При всьому при тому подібні пристрої мали і суттєві недоліки, які не дозволено було відрізнити неправильне спрацьовуванню від тривожного без участі людини, а при тривожній події часто не дозволено було йому запобігти, при цьому, при сильному завантаженні мережі SMS-повідомлення могло бути доставлено із запізненням від декількох хвилин до декількох годин, що робило цю систему непотрібною. Сучасні системи відеоспостереження по GSM зазвичай виконують такі функції: взаємодія користувача з пристроєм для отримання відео зображення може проводитися в будь-який час; ви вимкнули передачу відео від 1-4 телекамер в реальному часі (затримка від початку події аж до відображення на приймальному моніторі не більше 1-2 сек); автоматичний дозвон аж до користувача по спрацьовуванню вбудованого детектора руху і / або весняного датчика; автоматичний запис фото і відеоінформації у вбудовану пам'ять пристрою; запис прийнятої фото і відеоінформації на жорсткий диск комп'ютера; підключення зовнішнього охоронного датчика або шлейфа до тривожного входу пристрою; підключення виконавчого пристрою до релейного виходу пристрою і пряме управління ним по каналу зв'язку.Застосування систем віддаленого відеоспостереження по GSM ймовірно на віддалених об'єктах, де відсутні провідні канали зв'язку: заміські будинки, дачі, склади, автостоянки, гаражі, автозаправні станції, залізничні переїзди. Для віддаленого відео контролю за комунікаціями: водо-, газо- і нафтопроводи, електростанції, окремо які стоять підстанції, вишки тощо. Незважаючи на уявну складність пристроїв відеоспостереження по GSM, вони залишаються прості в підключенні і комфортні в експлуатації. Вже не потрібно використання на передавальній стороні мобільного телефону, GSM-модуль вбудований прямо в остов приладу. Електроживлення здійснюється від джерела постійного струму з широким діапазоном напруг 8-15В або від електромережі 220В.Альтернативою GSM-каналу є бездротові мережі WLAN (Wireless Local Area Network - бездротова локальна мережа). Мережа WLAN - вид локальної обчислювальної мережі (LAN), що використовує для зв'язку і передачі даних між вузлами високочастотні радіохвилі, а не кабельні з'єднання.

Призначені для користувача пристрої можна інтегрувати в мережу, встановивши на них бездротові мережні адаптери. Для забезпечення бездротовим користувачам доступу до вже існуючої мережі Ethernet потрібно встановити бездротову точку доступу. Найбільш важливий елемент бездротових мереж - бездротова точка доступу (англ. Wireless Access Point)

Точки доступу покликані виконувати найрізноманітніші функції, як для підключення групи комп'ютерів (кожен з бездротовим мережним адаптером) в самостійні мережі, так і для виконання функції моста між бездротовими і кабельними ділянками мережі. Такі суміщені мережі називаються Інфраструктурою і використовуються для доступу до центральних баз даних або бездротового підключення мобільних користувачів.

Рис. 1.2. Схема побудова відеосистеми на WI-FI

Cтандарт Wi-Fi (англ. Wireless Fidelity - "бездротова точність", за аналогією з Hi-Fi - стандарт на обладнання Wireless LAN). При використанні сучасних потокових алгоритмів стиснення швидкості 0,5 Мбіт / с цього цілком достатньо для передачі одного каналу відео пристойної якості. Також яку можна збільшувати за допомогою спрямованих антен і проміжних точок доступу (рис1.2).

Захист відеоінформації в бездротових IР-системах відеоспостереження досягається декількома способами. Ключовими серед них є: застосування брандмауерів, використання паролів і шифрування. Брандмауер працює як електронні "ворота", пропускають зареєстрованих користувачів і забороняють доступ неавторизованих особам. Застосування паролів дозволяє не тільки обмежити доступ до системи відеоспостереження, а й розподілити права доступу персоналу до певних відеокамер. А при шифруванні спроби перехоплення зашифрованих даних в IP-системі охоронного відеоспостереження стають безглуздими, якщо зловмисник не знає унікального коду для розшифровки потоку даних. Код, в свою чергу, встановлюється системним адміністратором.

 GPS моніторинг транспорту.

 Супутниковий моніторинг транспорту - система супутникового моніторингу та управління рухомими об'єктами, побудована на основі використання сучасних систем супутникової навігації (GPS / ГЛОНАСС), обладнання та технологій зв'язку (GSM / УКВ), обчислювальної техніки і цифрових карт. GPS моніторинг транспорту - технологія, що застосовується в диспетчерських службах на транспорті, а також для вирішення завдань транспортної логістики в системах управління перевезеннями (англ. TMS - Transportation management system) і автоматизованих системах управління автопарком (англ. FMS - Fleet Management System) для контролю фактичних маршрутів транспортних засобів за допомогою системи GPS.

Автотрекер - прилад, який встановлюється на автомобіль з метою відстеження його подальшого переміщення та контролю його місця розташування.

Зазвичай автотрекер визначає своє місце розташування приймаючи сигнали ГЛОНАСС / GPS і відправляючи їх за допомогою мобільного інтернет каналу GPRS на сервер в інтернеті, на якому власник приладу спостерігає його переміщення. Майже всі сучасні (2008-2009 рр.) прилади, що працюють на цьому принципі, можуть приймати вхідні дзвінки.

Для вирішення завдань моніторингу використовуються наступні компоненти системи:

- супутникові системи навігації (GPS - США, ГЛОНАСС - РФ),

- приймачі GPS і / або ГЛОНАСС,

- системи зв'язку з центральним пунктом (космічна / GSM / УКВ) і / або система локального накопичення даних.

 Іноді додатково використовуються додаткові датчики, встановлені на самому технічному засобі: поточний запас палива, факт відкриття дверей або капота, факт наявності пасажира (таксі), температура в рефрижераторі, факт роботи або простою спецмеханізмів (поворот стріли крана, роботи бетонозмішувача), факт натискання тривожної кнопки і т.п.

Отримані дані можуть або накопичуватися в локальному пристрої і потім переноситися в центральну базу після повернення в парк, або передаватися на центральний сервер в режимі реального часу.

Системи GPS моніторингу транспорту вирішують наступні завдання:

- моніторинг включає відстеження поточних координат, напрямку і швидкості руху транспортного засобу в реальному часі для потреб диспетчерських служб. У деяких системах також можлива установка додаткових датчиків на відкриття дверей, включення / вимикання виконавчих механізмів спецтехніки, паливних датчиків, датчиків для вимірювання температури в рефрижераторі та ін. Деякі системи допускають підключення до бортового комп'ютера автомобіля (через CAN-шину) і віддалене читання параметрів експлуатації транспортного засобу:

- облік пройденого кілометражу і витрати палива потрібен для своєчасного проходу ТО, обґрунтування списання ПММ бухгалтерією та ін. В системах TMS за допомогою GPS проводиться автоматичний облік доставки вантажів в задані точки.

- контроль відповідності фактичного маршруту автомобіля плановому дозволяє підвищити дисципліну водіїв. В Україні, на відміну від розвинених країн, ця функція вкрай затребувана для припинення несанкціонованого використання службових транспортних засобів найманими водіями з метою особистого збагачення, а також для припинення несанкціонованого зливу палива. За оцінками журналу «Логістика», тільки за рахунок підвищення дисципліни водіїв в російських умовах системи GSM моніторингу окупаються за кілька місяців.

- безпека: знання координат дозволяє швидко знайти викрадене або потрапило в біду транспортний засіб. Додатково автомобілі можуть бути обладнані прихованою кнопкою, натискання або не натискання на яку відсилає тривожний сигнал в диспетчерський центр. Крім цього, деякі термінали GPS моніторингу можуть працювати в режимі GSM-сигналізації, тобто дзвонити на заданий телефонний номер в разі спрацювання штатної сигналізації.

 Типова система GPS моніторингу складається з трьох ланок: терміналів, що встановлюються на автомобілі, сервера і клієнтських робочих місць. Термінали представляють собою спеціалізовані GPS-трекер, що містять модуль власне GPS і модуль стільникового зв'язку (GSM або CDMA). Функції сервера може виконувати звичайний ПК з встановленим серверним ПЗ. На відміну від робочих місць, сервер повинен бути завжди включений, так як саме на ньому накопичуються дані про маршрути. Клієнтське ПЗ в рідкісних випадках може бути об'єднано в одну програму з серверною частиною, але як правило допускається одночасне підключення декількох робочих місць до одного сервера.

Залежно від застосовуваних технічних рішень можна виділити п'ять поколінь систем GPS моніторингу транспорту:

- найперші системи були оффлайновими, тобто не дозволяли здійснювати моніторинг в реальному часі. GPS-трекер записував всі дані в пам'ять і передавав їх на сервер після прибуття транспортного засобу на базу через провідний або безпровідний інтерфейс. Така схема дозволяла контролювати маршрут автомобіля тільки постфактум і не здатна допомогти, наприклад, при викраденні автомобіля.

- у другому поколінні для організації зв'язку між GPS-терміналами та сервером використовувалися SMS або механізм CSD. На сервер встановлювалися один або кілька модулів стільникового зв'язку, що дозволяють приймати SMS або дзвінки з даними. Подібні системи відрізнялися величезними платежами за мобільний зв'язок і дуже великим періодом часу між вимірами координат. З масовим поширенням мобільного інтернету системи другого покоління практично вимерли.

- в третьому поколінні в якості транспортної мережі використовуються GPRS або EV-DO, що дозволяє на порядок знизити витрати на мобільний зв'язок і різко поліпшити точність промальовування маршрутів. Сервер в таких системах встановлюється безпосередньо у клієнта і підключається до інтернету і до локальної мережі офісу. На сервер і на робочі місця користувачів встановлюється спеціалізоване програмне забезпечення. У деяких системах допускається оренда портів сервера, що надає постачальник. На даний момент це найпоширеніша схема моніторингу.

- системи четвертого покоління також використовує один з механізмів мобільного інтернету в якості транспортної системи, але відрізняються від третього використанням веб-технологій. У цьому випадку сервер розміщується у компанії-постачальника, його потужності діляться між багатьма клієнтами, а захищений доступ до даних здійснюється через Web-сторінку з будь-якого комп'ютера, підключеного до інтернету. Так як один сервер здатний працювати одночасно з тисячами трекерів, різко знижується вартість впровадження і обслуговування системи. Одночасно зростає надійність зберігання і доступність даних, так як компанії-оператори здатні містити багато разів резервувати якісне серверне обладнання і штат технічних фахівців для його цілодобового обслуговування. Потенційним недоліком систем четвертого покоління є повна централізація - ймовірність збою або настання форс-мажорних обставин в таких системах є вкрай низькою, зате наслідки збою можуть стати дуже дорогими для компанії-оператора.

- системи моніторингу п'ятого покоління являють собою глобальний розвиток і централізацію систем попереднього покоління в єдиний, розподілений центр моніторингу. У такому варіанті дані від пристроїв збираються одним або декількома комунікаційними серверами, стікаються на один основний сервер бази даних і розтікаються між підключеними проміжними серверами, які вже забезпечують взаємодію з користувачем (веб-моніторинг) або виконують фонові завдання. При такій побудові системи користувачі з різних районів, країн і навіть континентів працюють з найближче розташованих регіональним веб-сервером з мінімальною затримкою (пінгом) до нього.

 На даний момент на українському ринку представлено близько 20 різних систем GPS моніторингу, як імпортних, так і вітчизняних. Імпортні рішення, як правило, відрізняються розширеною функціональністю, зате в вітчизняних краще реалізовані функції контролю за несанкціонованим використанням автомобіля, краще вирішене питання карт, а форми звітів відповідають російським законодавством. Важливим фактором є також захист терміналів від протидії водіїв: наявність резервного акумулятора, пломбування пристроїв та інші.

 В якості основного каналу зв'язку в професійних СКУД можуть використовуватися тільки ті бездротові технології, які еквівалентні по функціоналу, призначенням і вартості наявних у звичайній наземній комп'ютерної мережі підприємства, - це Wi-Fi, Wi-Max і аналогічні бездротові мережі.

Технології сенсорних мереж типу ZigBee, Z-Wawe і інші аналогічні повинні використовуватися за своїм прямим призначенням - для отримання інформації від різних датчиків без прокладання проводів на обмеженій (локальній) території. Така приваблива мережа як GSM, може використовуватися або в домашніх системах, або як додатковий канал віддаленого доступу до сервера СКУД для отримання звітів і аналогічних дій.

1.4. Огляд існуючих систем безпеки, що використовують gsm канали

Радіосистема «Стрілець».

Радіосистема «Стрілець» - одна з перших вітчизняних радіосистем, призначена для організації охоронно-пожежної та адресно-аналогової пожежної сигналізації на об'єктах не тільки приватного, а й громадського користування, де з різних причин (збереження цілісності інтер'єру, безперервна експлуатація приміщень і т.д .) застосування дротових систем неможливо або обмежене.

Особливості системи:

- двосторонній протокол обміну між усіма радіопристроями Аргус-Діалог;

- 10 радіочастотних каналів передачі (з автоматичним і ручним вибором);

- автоматичний вибір резервного каналу передачі (вільного від перешкод);

- рознесений радіоприйом;

- до 400 радіопристроїв, які перебувають в зоні взаємної радіовидимості на одному радіочастотному каналі передачі.

- можливість побудови повноцінної адресної пожежної радіосистеми.

- програмований період передачі контрольних радіосигналів від 12 с до 2 хв.

- криптографічний захист сигналів з механізмом динамічної аутентифікації.

- мікростільникова топологія системи.

Ємність системи:

- до 16 радіо розширювачей

- до 512 радіооповіщувачів (до 32 оповіщувачів на кожен радіо розширювач)

- до 256 радіоканальних виконавчих пристроїв, сирен, брелків і пультів управління (до 16 пристроїв на кожен радіо розширювач).

дальність:

- до 600 м в межах мікростільники

- до 1000 м між мікросотами

- до 6000 м - 5 ділянок ретрансляції.

Тривалість роботи радіооповіщувачів:

- від основної батареї: від 3 (період передачі контрольних радіосигналів 12 с) до 7,5 років (період передачі контрольних радіосигналів 2 хв.);

- від резервної батареї: не менше 2 місяців.

Система має два діапазони робочих частот: 433 МГц або 868 МГц

Передбачена інтеграція радіосистеми СТРЕЛЕЦ® з бездротовою системою "Орфей-Р". Для побудови повноцінної системи охорони існує можливість інтеграції радіосистеми Стрілець з відомою системою відеоспостереження "Відеоінтелект". Для передачі повідомлень з об'єктів на централізовані пульти охорони, в тому числі і ЧОП, передбачена спільна робота радіосистеми Стрілець з популярними СПС "Андромеда", "Міраж".

Також існує можливість інтеграції радіосистеми Стрілець з системою контролю і управління доступом (СКУД) "Кронверк" і апаратно-програмним комплексом "Бастіон".

Мікростільникова структура радіосистеми Стрілець дозволяє зв'язати в єдину систему ОПС групу окремо розташованих об'єктів, надавши можливість як централізованого (з поста охорони), так і децентралізованого (на кожному об'єкті) контролю і управління системою.

Розглянемо РСПІ «Дельта».

РСПІ "Дельта" призначена для забезпечення передачі інформації з охоронюваних віддалених об'єктів, її збору, обробки та зберігання на пультах централізованого спостереження в масштабах підприємств, районів, міст, областей. Забезпечується: пожежна, охоронна, тривожна сигналізація, контроль доступу на об'єкти, що охороняються, автоматичний контроль стану обладнання, контроль стану і витоку хімічно небезпечних речовин, витоку води, газу, телеметрія і т.д. Сповіщення, що посилаються об'єктовими передавачами, надходять на пульти централізованого спостереження. Кожне прийняте повідомлення декодується і обробляється, після чого оператор може вжити необхідних заходів щодо залучення сил швидкого реагування. Передбачено дублювання по телефонних лініях і автоматична відправка SMS повідомлень. Принцип роботи радіо канальної системи передачі сповіщень "Дельта" заснований на використанні виділеного для цих цілей радіочастотного ресурсу для передачі повідомлень з об'єктів, обладнаних радіопередавачами, на пульт централізованого спостереження, де відбувається прийом повідомлень, їх обробка, відображення на моніторі диспетчера, який передає отриману інформацію в відповідні служби реагування по спеціальних каналах зв'язку.

Використання виділеного каналу виключає залежність системи від інших операторів зв'язку, а його експлуатаційна готовність забезпечується державною радіочастотної службою. До об'єктового радіопередавачу може бути підключена будь-яка периферія (охоронна, тривожна, пожежна сигналізація, датчики витоку води, газу, телеметрія і т.д.).

Конфігурація мережі дозволяє використовувати інформацію, необхідну для відповідного реагування таким структурам, як підрозділи позавідомчої охорони МВС, відомча охорона, служба порятунку, пожежна охорона, приватні охоронні підприємства, міські комунальні служби, підприємства водопостачання. електромережі, тепломережі тощо

Основні характеристики:

 - Частотний діапазон 136-174 або 400-500 МГц.

 - Потужність передавачів до 15Вт.

 - Дальність без ретрансляції 15 км.

 - До 30 ретрансляторів в системі.

 - Ємність системи 12000 об'єктів з використанням однієї частот.

Склад системи:

- пульти централізованого спостереження, що складаються з: АФП - антенно-фідерних пристроїв, базових станцій, ПК - персональних комп'ютерів з встановленим ПЗ АРМ - програмним забезпеченням автоматизованого робочого місця операторів, обладнання енергонезалежного живлення. Для автоматичної відправки SMS повідомлень використовуються спеціалізовані GSM радіомодеми - "Дельта GSM". Дублювання по телефонній лінії забезпечує "Дельта-Т".

- об'єктове обладнання складаються з передавачів з антенами, підключених до сповіщувачів безпосередньо або до будь-яких ПКП - приймально контрольних приладів і обладнання енергонезалежного живлення.

-для розширення зони радіо охорони можуть використовуватися ретранслятори.

Основні відмінні риси:

- велика дальність забезпечена високою потужністю передавачів - до 15 Вт і високою чутливістю приймального тракту -0.25мкВ.

- велика ємність, забезпечена малою тривалістю посилки - 0.125 секунди

- передавачі виконують функції об'єктових ПКП.

- застосування високошвидкісного формату FSK передачі даних з перевіркою контрольних сум повідомлень і алгоритм дублювання повідомлень, що передаються з рознесеними по часу посилками в випадковий часовий інтервал (5-8 секунд) надають системі високу надійність при високій ємності і інформативності (до 256 параметрів).

 - інтервал тестових сигналів може бути встановлений від 1 хвилини до 256 годин, що дозволяє тестувати об'єкти з необхідним періодом в залежності від ємності системи або в залежності від категорії об'єктів.

- одночасний моніторинг стаціонарних і мобільних об'єктів.

- комплексне використання прямого радіоканалу, телефонних каналів і GSM.

- невисока вартість.

- можливість побудови системи від невеликого пульта з декількома об'єктами, що охороняються до мережі, що включає в себе велику кількість центральних станцій і ретрансляторів, в масштабах великого міста або області.

Системи «Дельта "використовують протоколи, подібні системі" PIMA "(Ізраїль) і" Informer 12000 "(США), що дозволило перейняти більш багатий досвід світових лідерів і при цьому мати всі переваги вітчизняного виробника.

Розглянемо як приклад «Орлан GSM 900/1800» ( «Охорона та безпека», Україна)

 «Орлан» - комплекс технічних засобів і програмного забезпечення для створення ПЦС за станом пристроїв пожежної та охоронної сигналізації GSM з використанням мережі GSM-900/1800 в голосовому режимі і режимі GPRS. Призначений для прийому кодованих повідомлень, переданих радіокоммунікаторами серії «Лунь», і трансляції їх на ПК для реєстрації та обробки за допомогою програмного забезпечення «Фенікс 2». Програмне забезпечення підтримує підключення до ПК цифрових приймачів ПАКТ2 і DSC-SurGard для прийому кодованих повідомлень по телефонній лінії від більшості охоронно-пожежних панелей (Napco, Ademco, DSC і ін.). ПЦС «Орлан» можна отримувати інформаційні повідомлення від зовнішніх пристроїв зі звуковим і візуальним супроводом, розшифровкою і обробкою, стеження і миттєвою зміною стану об'єкта на ПЦС при приході чергового повідомлення. Передбачено до п'яти функцій віддаленого управління об'єктовими приладами операторами пульта, а також зберігання і відображення інформації в текстовому і графічному вигляді.

 ПЦС веде архіви прийнятих повідомлень, пошук в архіві за різними критеріями, друк і експорт бази даних, архіву подій. Є можливість розбивки об'єкта на групи і відстеження інформації окремо по кожній групі, можливість завдання розкладу роботи для кожної з груп. Резервне копіювання та архівування бази даних відбувається автоматично. Дублювання. Всі події з об'єкта дублюються на мобільний телефон господаря у вигляді SMS (до 3 телефонів), на віддалений пульт «Фенікс-міні» у вигляді SMS (до 3 пультів), а також по каналу GPRS. Є можливість переведення об'єкта, групи або окремого шлейфа в режим постійного або тимчасового стенду. Проводяться аналіз і побудова графіків і звітів про роботу пульта за місяць. Інформативність (види повідомлень) - 256. Розмір буфера пам'яті прийнятих подій - 32. Час готовності ПЦС до роботи - не більше 40 секунд. Час одного сеансу зв'язку в голосовому режимі - не більше 4 секунд. Час одного сеансу зв'язку в в режимі GPRS - не більше 1 секунди.

Централізована база даних в форматі Microsoft SQL Server 2000 з клієнт-серверною архітектурою ПЗ, розподілений доступ до БД з різних ПК в мережі. Протоколювання часу прибуття групи реагування на об'єкт. Індивідуальний інтервал тестування для кожного охоронного приладу (від 15 хв.). Реєстрація операторів ПЦС.

 Розглянемо СПС Андромеда.

 СПС Андромеда має п'ять каналів передачі інформації: радіо, телефонної лінії, GSM (GPRS, SMS, Voice), LAN / WAN, можливість підключення до 8000 об'єктів, відображати на карті міста об'єкти і групи швидкого реагування в реальному часі. Безліч корисних функцій спрощують і автоматизують роботу операторів. Для роботи з GSM-каналу застосовується комплект об'єктових пристроїв системи «Андромеда Hunter-Pro 96». Цей об'єктовий прилад має розширення до 96 зон і з можливістю передачі сигналу по всіх каналах зв'язку. Модуль стільникового зв'язку GSM-200 забезпечує передачу повідомлень від контрольної панелі на центральну станцію в голосовому каналі та каналі GPRS стандарту GSM.

 У СПС Андромеда вирішено взаємодія з пультами виробництва компанії «Альтанка» (системи LONTA®-202 і «Риф-Стрінг» -200), а так само з пультами, що мають на виході відкриті стандартні протоколи «Sur-Gard» (власне пульти «Sur -Gard », пульт« Контакт-GSM », виробництва ТОВ« Ритм ») і« Ademco 685 »(наприклад, LARS).

Для використання інших сучасних каналів зв'язку (Ethernet, GPRS) також цілком достатньо доопрацювання використовуваного на ПЦС програмного забезпечення. У СПС Андромеда також інтегрована система Стрілець за допомогою перетворювача «СТЕЛС». Це самостійний прилад, що забезпечує підключення до 16 РРОП, які збирають інформацію від датчиків і передають її в центр моніторингу. Оскільки кожен РРОП може обслуговувати до 32-х датчиків, отримуємо систему, яка дозволяє передавати повідомлення з об'єкта, обладнаного 512 різними бездротовими пристроями, що входять до складу системи Стрілець. СПИ Андромеда має п'ять каналів передачі інформації: радіо, телефонної лінії, GSM (GPRS, SMS, Voice), LAN / WAN, можливість підключення до 8000 об'єктів, відображати на карті міста об'єкти і групи швидкого реагування в реальному часі. Безліч корисних функцій спрощують і автоматизують роботу операторів. Для роботи з GSM-каналу застосовується комплект об'єктових пристроїв системи «Андромеда Hunter-Pro 96». Цей об'єктовий прилад має розширення до 96 зон і з можливістю передачі сигналу по всіх каналах зв'язку. Модуль стільникового зв'язку GSM-200 забезпечує передачу повідомлень від контрольної панелі на центральну станцію в голосовому каналі та каналі GPRS стандарту GSM. У СПИ Андромеда вирішено взаємодія з пультами виробництва компанії «Альтанка» (системи LONTA®-202 і «Риф-Стрінг» -200), а так само з пультами, що мають на виході відкриті стандартні протоколи «Sur-Gard» (власне пульти «Sur -Gard », пульт« Контакт-GSM », виробництва ТОВ« Ритм ») і« Ademco 685 »(наприклад, LARS). Для використання інших сучасних каналів зв'язку (Ethernet, GPRS) також цілком достатньо доопрацювання використовуваного на ПЦС програмного забезпечення. У СПИ Андромеда також інтегрована система Стрілець за допомогою перетворювача «СТЕЛС». Це самостійний прилад, що забезпечує підключення до 16 РРОП, які збирають інформацію від датчиків і передають її в центр моніторингу. Оскільки кожен РРОП може обслуговувати до 32-х датчиків, отримуємо систему, яка дозволяє передавати повідомлення з об'єкта, обладнаного 512 різними бездротовими пристроями, що входять до складу системи Стрілець.

Станція моніторингу STAM-2 (Satel, Польща).

Станція моніторингу STAM-2 польської компанії Satel складається з програмного забезпечення, основної плати для прийому повідомлень від ПКП і захисного апаратного USB-ключа. При цьому основну плату можна встановити в будь-який вільний PCI-слот ПК, а c автономним джерелом живлення можлива робота станції й без комп'ютера. Програма моніторингу істотно полегшує роботу оператора системи ОПС, автоматично вибираючи події, що вимагають його втручання, надаючи список інструкцій в кожній конкретній ситуації і нагадуючи про невиконані завдання. STAM-2 може обслуговувати понад 50 000 абонентів, виводити на друк звіти про дії операторів системи ОПС, звіти про системні події і автоматично відстежувати несанкціоновану зміну системних файлів.

ПЦС STAM-2 підтримує такі способи обміну даними з ПКП: прийом сигналів по телефонній лінії, по IP-каналу, по мережі GSM у вигляді SMS-повідомлень і по радіоканалу при наявності радіостанції стандарту VISONIC. При цьому підбір плат, встановлених на ПК, залежить від обраних 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.

 Система має модульний принцип побудови. Один модуль «АРМ оператора ПЦС» дозволяє підключити до 540 об'єктів. Можна організувати роботу кількох «АРМ оператора ПЦС». В якості комунікатора використовуються універсальний комунікатор (GSM + ГТС) і IP-комунікатор (IP-модем). По каналу GSM інформація передається в цифровому форматі DATA.

SMS-повідомлення власника об'єкта про доставку повідомлення на ПЦС і на стільниковий телефон власника. Альтернативний канал передачі сповіщень між контактами реле ПЦС.

ПЦС є автоматизоване робоче місце на основі персонального комп'ютера з підключеними до нього концентраторами і встановленим програмним забезпеченням інтегрованої системи безпеки «Лавина».

Дозволяє вирішувати комплекс завдань з моніторингу системи, підготовки і ведення бази даних по об'єктах, програмування ключів перенесення даних для об'єктових приладів. Можливо виконання адаптивної конфігурації та налаштування системи, програмування об'єктових приладів, отримання різної довідкової та звітної інформації. Програмне забезпечення складається з декількох модулів, які забезпечують прийом і декодування інформації, відображення стану всіх об'єктів, підключених до системи, видачу тривожних сповіщень, фіксацію дій операторів при надходженні тривожних повідомлень, детальне уявлення кожного об'єкта; відображення журналу подій, контроль працездатності модулів зв'язку з концентратором.

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

 Програмована бездротова сигналізація ABAX.

 Система ABAX включає в себе бездротові контролери, охоронні датчики, сповіщувачі та інші пристрої ОПС фірми Satel, на базі яких будується система бездротового сигналізація офісу, магазину або квартири. Ця система дозволяє розширити бездротовими пристроями будь-яку дротову ОПС. Важливою особливістю ABAX є наявність двостороннього радіозв'язку між контролером і пристроєм захисту даних, що забезпечує високу ступінь захисту системи ОПС від злому і саботажу.

 ABAX моментально реагує на тривожні події і передає тривогу на ПКП системи. При цьому вона забезпечує роботу системи сигналізації в енергозберігаючому режимі і дозволяє дистанційно конфігурувати бездротові пристрої за допомогою русифікованого ПЗ. Працює ABAX в смузі частот 868,0 ... 868,6 Гц з модуляцією FSK.

 В якості базового пристрою сигналізації ABAX використовується контролер ACU-100 фірми Satel, який може обслуговувати одночасно до 48 охоронних пристроїв, і працює спільно з будь-якими приймально-контрольними приладами (ПКП). ABAX організовує двосторонній зв'язок між бездротовими пристроями, тому прийом повідомлень від датчиків сигналізації завжди підтверджується. У той же час ACU-100 проводить в режимі on-line опитування бездротових датчиків сигналізації, визначаючи присутність в системі кожного пристрою.

 Система моніторингу рухливих об'єктів "Алмаз".

 Призначена для захисту і моніторингу мобільних, а також стаціонарних об'єктів з використанням технології ГЛОНАСС / GPS / GSM. Відмітна особливість системи - наявність другого (резервного) каналу зв'язку, який організовується на базі УКХ-зв'язку або супутникового телефону.

 Система моніторингу рухливих об'єктів "Алмаз" служить для організації централізованої охорони і моніторингу рухомих (стаціонарних) об'єктів на базі технологій GPS / GSM, а також підвищення оперативності управління групами затримання підрозділів позавідомчої охорони.

 Відповідно до призначення в числі основних функцій системи:

- стеження за місцем розташування контрольованих рухомих об'єктів з використанням електронної карти місцевості;

- контроль, диспетчеризація і охорона автотранспорту та інших рухомих об'єктів;

- контроль стану датчиків об'єкта, підключених до термінальних пристроїв, і ситуацій на об'єктах;

- фіксація позаштатних ситуацій на контрольованих об'єктах;

- управління виконавчими пристроями об'єктів при виникненні нештатних ситуацій;

- документування та архівування інформації, що надходить від об'єктів контролю і диспетчерського центру;

- організація надійних каналів зв'язку між диспетчерським центром та об'єктами контролю.

 Принцип дії системи заснований на комплексному використанні каналів системи стільникового зв'язку стандарту GSM 900 / DCS 1800 або радіоканалів УКХ в якості засобів обміну інформацією між абонентами системи і диспетчерським центром (ДЦ), а також глобальної системи позиціонування GPS для отримання інформації (визначення координат) про поточний місцезнаходження рухомих абонентів системи. Інформація від віддалених терміналів надходить в ДЦ для відображення, накопичення та подальшої обробки по каналах зв'язку стандарту GSM 900 / DCS 1 800 (із застосуванням послуг SMS або GPRS) і УКВ радіоканалах.

 Система "Алмаз" являє собою сукупність мережі термінальних пристроїв (ТУС), розташованих на рухомих і стаціонарних об'єктах, і диспетчерського центру моніторингу.

 До складу термінальних пристроїв, що встановлюються на борту автотранспортних засобів ( "Топаз-201"), входить приймач сигналів глобальної мережі позиціонування. Використовувана в системі "Алмаз" технологія обробки і передачі сигналів позиціонування рухомих об'єктів дозволяє з єдиного диспетчерського центру здійснювати моніторинг і управління об'єктами, відображати їх місце розташування на карті місцевості з точністю до 5 м.

 Система "Алмаз" забезпечує вирішення наступних завдань:

- контроль технологічних параметрів мобільних (стаціонарних) об'єктів і управління виконавчими пристроями цих об'єктів;

- управління парком транспортних засобів;

- охорону, управління і контроль мереж торгових автоматів або банкоматів;

- охорону об'єктів (житлових або службових приміщень, газопроводів, об'єктів енергомереж, автотранспорту та вантажів, що перевозяться).

 2. Дослідження систем безпеки, що використовують gsm канали

 2.1. Організація систем безпеки на основі gsm- каналів

 Стандарт GSM розроблений Європейським інститутом телекомунікаційних стандартів (ETSI) є одним з найбільш надійних і масових по використанню в засобах телекомунікації та зв'язку. Функціональна побудова і інтерфейси, прийняті в стандарті GSM показані на структурній схемі, де MSC (Mobile Switching Centre) - центр комутації рухомого зв'язку; BSS (Base Station System) - обладнання базової станції (БС); ОМС (Operations and Maintenance Centre) - центр управління та обслуговування; MS (Mobile Stations) - рухливі станції (МС).



 Рис. 2.1. Функціональна побудова і інтерфейси стандарту GSM

 Функціональне поєднання елементів системи здійснюється рядом інтерфейсів і показано на рисунку 2.1. Центр комутації мобільного зв'язку обслуговує групу сот і забезпечує всі види з'єднань, яких потребує в процесі роботи MSC. Він забезпечує як маршрутизацію викликів, так і функції управління викликами. Крім виконання функцій звичайної комутаційної станції ISDN MSC виконує і функції комутації радіоканалів. Кожен MSC забезпечує обслуговування рухливих абонентів, які знаходяться в межах певної географічної зони, а також підтримує процедури безпеки, які застосовуються для управління доступами до радіоканалів.

HLR - довідкова база даних про постійно прописаних в мережі абонентах. У ній містяться розпізнавальні номера та адреси, а також параметри автентичності абонентів, склад послуг зв'язку, спеціальна інформація про маршрутизації.

VLR містить такі ж дані, як і HLR, проте ці дані містяться в VLR тільки до тих пір, поки абонент знаходиться в зоні, контрольованій VLR. У мережі рухомого зв'язку GSM стільники групуються в географічні зони (LA), яким присвоюється свій ідентифікаційний номер (LAC). Кожен VLR містить дані про абонентів декількох LA. У разі якщо рухливий абонент переміщається з однієї LA в іншу, дані про його місцезнаходження автоматично оновлюються в VLR.

EIR - регістр ідентифікації встаткування, містить централізовану базу даних для підтвердження автентичності міжнародного ідентифікаційного номера обладнання мобільної станції (ІМЕІ).

ОМС - центр експлуатації і технічного обслуговування, є центральним елементом мережі GSM, який забезпечує контроль і управління іншими компонентами мережі та контроль якості її роботи. ОМС з'єднується з іншими компонентами мережі GSM каналами пакетної передачі протоколу Х.25.

NMC - центр управління мережею, що дозволяє забезпечувати раціональне ієрархічне управління мережею GSM. Він забезпечує експлуатацію і технічне обслуговування на рівні всієї мережі, підтримуваної центрами ОМС, які відповідають за управління регіональними мережами.

BSS - обладнання базової станції, складається з контролера базової станції (BSC) і приймально-передавальних базових станцій (BTS). Контролер базової станції може керувати кількома приймально-передавальними блоками.

 Використання персонального ідентифікаційного цифрового коду - один з простих методів аутентифікації. Він дає дуже низький рівень захисту в умовах використання радіозв'язку, тому крім нього GSM використовує більш складний метод, що складається в використанні випадкового числа, на яке може відповісти тільки відповідне абонентське обладнання. Шифрування для захисту конфіденційності є досить ефективним, але для захисту кожного окремо взятого обміну інформацією по радіоканалу не застосовується.

 Досить широке поширення на ринку систем безпеки в нашій країні отримав тип сигналізацій, що використовує функцію SMS повідомлень, що обумовлюється низькою вартістю і простотою використання даних GSM-сигналізацій. Даний тип передачі сповіщень використовується в основному як сервісний канал (в професійних охоронних системах). Оповіщення про тривожну ситуацію або про проникнення на об'єкт є обов'язковим атрибутом систем охорони і з точки зору технічної реалізації може бути виконано в такій формі як попередження голосом (дзвінком на телефон), DTMF - кодом [1], в будь-якому цифровому вигляді, а також передачею SMS повідомлення власнику. Текст може складатися з алфавітно-цифрових символів, максимальний розмір повідомлення в стандарті GSM - 140 байт. Таким чином, при використанні 7-бітної кодування (латинський алфавіт і цифри) можна відправляти повідомлення довжиною до 160 символів. При використанні 8-бітної кодування (німецька, французька мова) можна відправляти повідомлення довжиною до 140 символів. Для підтримки інших національних алфавітів (китайського, арабського, російського і ін.) Використовується 2-байтная кодування UTF-16 (Unicode). Таким чином, SMS-повідомлення, написане кирилицею, не може перевищувати 70 знаків. Що вельми обмежує використання даного сервісу в охоронному устаткуванні.

Технологія SMS підтримується основними стільниковими мережами: GSM, NMT, D-AMPS, CDMA, також SMS-повідомлення на телефони можна відправляти з інтернету та інших мереж, для цього можна використовувати спеціальні програми, а також безпосередньо шлюзи мобільних операторів. У всіх подібних сигналізацій використовуються GSM-модеми. На об'єкті, що охороняється, встановлюється контрольна панель з GSM-модулем. Залежно від типу зв'язку з датчиками підключаються охоронно-пожежні датчики. У разі спрацювання одного з датчиків, на панель надходить сигнал, в разі замикання однієї з зон, контролер дає команду GSM-модему відправити SMS повідомлення по одному або декільком номерам, що зберігаються в пам'яті.

 Широке поширення в нашій країні отримали і так звані дачні охоронні сигналізації. Такі GSM-сигналізації найчастіше поєднують в собі охоронні функції та функції дистанційного керування виконавчими пристроями. У професійній охорони даний тип зв'язку застосовується обмежено, в основному як сервісний канал, наприклад, для підтвердження взяття об'єкта під охорону або контроль напруги мережі на об'єкті, а також як останній резервний канал.

Зазвичай в GSM-сигналізації для пультів централізованого спостереження (ПЦС) використовуються стандартні формати, наприклад протокол Contact ID. Сьогодні DTMF - найпоширеніший канал передачі даних, тому що формати даних, принцип передачі і приймальне обладнання повністю запозичено у проводового моніторингу. Використання DTMF форматів висуває додаткові вимоги до опрацювання звукового тракту GSM-модему через те, що аналого-цифрові перетворення тягнуть за собою спотворення при передачі сигналу і тому можуть відбуватися збої при прийомі звітів від об'єктового обладнання. На жаль, дана проблема досить часто зустрічається у обладнання, виробленого в нашій країні. Більшість систем контролюють передачу даних, запитуючи, чи потрібно приймати і сигнал не губиться в мережі, але значно збільшується час проходження сигналу.

 CLIP (Calling Line Identification Presentation).

 Цей метод заснований на сервісі оператора мобільного зв'язку по наданню інформації про номер абонента, що здійснює дзвінок. Приймальний пристрій зчитує номер абонента і відхиляє виклик, при цьому сам факт дзвінка від відомого в системі абонента і є підставою для реєстрації тривожної події. До переваг такого методу слід віднести відсутність плати за вихідний дзвінок, але інформативність такого повідомлення дуже мала.

Для підвищення інформативності можна встановити на ПЦС кілька GSM-модемів. Передавальний пристрій програмують таким чином, щоб по одній групі подій модем робив виклик на перший модем (тривоги), по іншій групі - на другий і т.д

GSM DATA / CSD (Circuit Switch Data).

Цифровий канал передачі даних на швидкості 9,6 кбіт / с. Цей метод характеризується практично 100% -ною вірогідністю доставки повідомлення. Час встановлення з'єднання становить близько 20 с. На відміну від передачі повідомлення в стандартному форматі Contact ID в голосовому каналі, протокол передачі в CSD не стандартизований (хоча може бути максимально наближений до CID), що не дозволяє використовувати передавачі одного виробника в системі іншого виробника.

 TCP / IP GPRS (General Packet Radio Service).

 Технологія пакетної передачі GPRS використовує в якості механізму доставки пакетів даних протоколи TCP / IP. У цьому випадку кожному з пристроїв мережі присвоюється унікальний IP-адресу. Існує два види IP-адресів: статичні (які можуть надаватися Інтернет-провайдерами або операторами стільникових мереж) і динамічні, які видає оператор при приєднанні до мережі GPRS на час сеансу зв'язку.

На практиці такий спосіб організації каналу передачі даних майже не зустрічається через складність отримання статичних IP-адрес у стільникових операторів для всіх віддалених пристроїв системи

Перешкодостійкість і перешкодозахищеність GSM каналу

 Перешкоди в радіоканалі можуть створюватися як за рахунок спотворень сигналу при його поширенні, так і при впливі зовнішніх джерел. Перший тип спотворень досить легко усувається. Перешкоди ж від зовнішніх джерел зменшуються за допомогою розширення спектра сигналу, що передається.

 Основна складність при побудові GSM каналу пов'язана з неможливістю забезпечити безперервність GSM / GPRS-зв'язку, що може призводити не тільки до переривання передачі даних, але і до зависання модему.

 Додатково до перерахованих методів, для підвищення завадостійкості застосовують багаторазове дублювання фрагментів переданих повідомлень в частотній або часовій області. Перешкодостійкість, в області радіо канальних пожежних і охоронних систем можна визначити наступним чином:

кількістю частотних діапазонів, в яких може працювати радіосистема; кількістю частотних каналів в кожному діапазоні;

можливістю автоматичного вибору резервних каналів;

наявністю автоматичного регулювання потужності випромінювання.

Відповідно до європейської класифікації існує три класи пожежних і охоронних дротових і радіо канальних систем:

клас А: низький ступінь ризику - об'єкти приватного користування (заміські будинки, квартири);

клас В: середній ступінь ризику - об'єкти громадського користування (магазини, навчальні заклади);

клас С: висока ступінь ризику - об'єкти державної важливості (музеї, історичні пам'ятки).

Ще одна важлива характеристика - здатність радіолінії працювати в умовах впливу організованих перешкод називається перешкодостійкістю.

Перешкодо захист розділяється на два класи:

1) просторовий перешкодо захист (за рахунок низького рівня бічних пелюсток прийомної антени, за якими діє перешкода, формування "нулів" діаграми спрямованості приймальної антени в напрямку на джерело перешкод);

2) сигнальний перешкодо захист за рахунок широкосмугових методів модуляції.

Принцип придушення заснований на постановці вузькополосної перешкоди приймальному каналу GSM-пристрою. На сьогоднішній день заглушувачів GSM-пристроїв досить багато і основне їхнє призначення заглушати мобільні телефони на нарадах, конференціях, бібліотеках, театрах і т.п. Однак зловмисники цілком можуть застосовувати їх і для негативних цілей.

Для зниження глушіння сигналу потрібно:

1. мати дублюючий канал для обміну важливою інформацією;

2. використовувати періодичний тест з об'єкта;

3. застосувати виносні антени.

Аналіз моделі GSM каналу щодо забезпечення необхідної зони покриття

На дальність радіозв'язку впливають такі чинники:

1. Місцезнаходження BS і MS і рельєф місцевості.

2. Потужність і чутливість MS.

3. Потужність і чутливість BS.

4. Використовувані на MS і BS антени.

Зазвичай базові станції мають потужність 20 - 30 Вт. Антени застосовуються або штирові, або спрямовані. Чутливість базових станцій становить - 100 дБ - 115 дБ.

Залізобетонні будови здатні послаблювати сигнали, що проходять через них (при внутрішньому покритті), в 100-1000 разів (тобто на 20-30 дБ). До числа перешкод можна також віднести кузова автомобілів, крони дерев і т.д. Вплив можуть надати і атмосферні опади.

При розрахунку зони покриття застосовується модель Хата, так як вона рекомендована Міжнародним Консультативним комітетом з Ради радіозв'язку (МККР) і досить проста в застосуванні. Ця модель дозволяє обчислити втрати на радіотрасі для конкретної місцевості і параметрів базової станції.

Середній рівень втрат на радіотрасі, слідуючи емпіричної моделі Хата, визначається наступним чином:

 

Де частота, (МГц); висота базової станції, (м);  відстань між базовою станцією і абонентською станцією, (км); висота абонентської станції, (м);

 коефіцієнт, що враховує висоту антени абонентської станції, (для невеликого або середнього міста,  для великого міста),



коефіцієнт, що враховує характер місцевості (для сільської місцевості, для передмістя, для міста),



- коефіцієнт, що відображає вплив щільності забудови

(%) - щільність забудови;



коефіцієнт, що враховує сферичність Землі (вводиться, якщо 0,2R0 <r ≤ 0,8R0, де R0 - відстань прямої видимості).

 Таким чином, використання вищеописаних систем безпеки для забезпечення збереження матеріальних цінностей різних форм власності є досить ефективними. У свою чергу ефективна охорона сьогодні немислима без використання різних технічних засобів, які дозволяють здійснювати цілодобову охорону об'єктів, максимально виключивши людський фактор, знизити витрати на її утримання і істотно підвищити її надійність.

Найпоширеніший канал передачі даних в охоронних системах використовує GSM технології передачі даних. Voice канал - це голосовий тракт використовує мовне оповіщення (зазвичай в приватних охоронних системах) і DTMF-код (обладнання для пультів централізованого спостереження).

 У разі тривоги GSM-сигналізація дзвонить Вам на телефон і промовляє в заздалегідь записане повідомлення.

 З DTMF трохи складніше. DTMF (Dual Tone Multi Frequency) - термін для позначення тонального набору. Синонімом цього терміна є слово Touchtone (широко не вживається, тому що Touchtone є зареєстрованим товарним знаком AT & T). У DTMF при натисканні на клавішу кнопкового телефону лунає звук (тон), який є комбінацією двох тонів, високо- і низькочастотного. Звідси і назва (Dual - подвійний)

 Система сигналів DTMF включає вісім тонів, які були спеціально підібрані таким чином, щоб передаватися через телефонну мережу без загасання і з мінімальним впливом один на одного. Оскільки ці звукові сигнали потрапляють в частотний діапазон людського голосу, були додатково введені заходи для того, щоб голос не сприймався як набір. Одна з таких заходів - розподіл тонів на дві групи, високо- і низькочастотну. Нижче наведена таблиця DTMF-тонів різних цифр (і керуючих клавіш) кнопкового телефону і відповідних їм пар частот. Один Герц (Гц) - це частота, що дорівнює одному коливанню в секунду.

|  |  |  |
| --- | --- | --- |
| **Цифра, символ**  | **Низька частота,** Гц  | **Висока частота,** Гц  |
| 1  | 697  | 1209  |
| 2  | 697  | 1336  |
| 3  | 697  | 1477  |
| 4  | 770  | 1209  |
| 5  | 770  | 1336  |
| 6  | 770  | 1477  |
| 7  | 852  | 1209  |
| 8  | 852  | 1336  |
| 9  | 852  | 1477  |
| 0  | 941  | 1336  |
| \*  | 941  | 1209  |
| #  | 941  | 1477  |

 Зазвичай в GSM-сигналізації для пультів централізованого спостереження (ПЦС) використовуються стандартні формати, наприклад протокол Contact ID. На даний момент DTMF - найпоширеніший канал передачі даних, оскільки формати даних, принцип передачі, приймальне обладнання - повністю запозичене у проводового моніторингу. Наприклад, якщо охоронне підприємство вже має станцію централізованого моніторингу, то застосування GSM-сигналізацій не викликає зайвих витрат, тому що не потрібно замінювати обладнання на станції моніторингу. Використання DTMF форматів висуває додаткові вимоги до опрацювання звукового тракту GSM-модему. Аналого-цифрові перетворення тягнуть за собою спотворення при передачі сигналу. Через це можуть відбуватися збої при прийомі звітів від об'єктового обладнання. Дана проблема досить часто зустрічається у вітчизняного обладнання. І хоча сигнал не згубиться в мережі (більшість систем контролюють передачу даних, запитуючи, чи потрібно приймати), але значно збільшиться час проходження сигналу. Причому збільшення часу проходження сигналу може бути фатальним. Уявіть собі ситуацію, коли на об'єкт встановлено обладнання використовує передачу даних в форматі DTMF кодів. Через несправність обладнання або поганої якості сигналу, об'єктовий прилад не зможе передати повідомлення на пульт. І, як наслідок, не отримає підтвердження про прийом. Не отримавши повідомлення про прийом прилад почне повторний набір, зі спробою передати повідомлення. Але в підсумку, не отримавши нічого, починається цикл дозвонів. Цей цикл повністю займе весь канал, що не дозволить передати повідомлення іншим об'єктовим приладів, тобто буде втрачено зв'язок з об'єктами. Чи не буде повідомлень про тривогу, що не буде повідомлень про постановку і зняття з охорони і т.д. І як наслідок повністю неробочий пульт централізованого спостереження. Так DTMF це дуже зручно і дешево (передача даних вкладається в 5 секунд), але які можуть бути від цього наслідки.

 2.2. Дослідження принципів шифрування gsm каналу

Використання пароля (або PIN-код - персонального ідентифікаційного цифрового коду) - один з простих методів аутентифікації. Він дає дуже низький рівень захисту в умовах використання радіозв'язку. Досить почути цей персональний код всього лише один раз, щоб обійти засоби захисту. Насправді GSM використовує PIN-КОД в поєднанні з SIM (Subscriber Identify Module): даний PIN-КОД перевіряється на місці самим SIM без передачі в ефір.



 Рис. 2.2. Обчислення аутентифікації

 Крім нього, GSM використовує більш складний метод, який полягає у використанні випадкового числа (від 0 до 2 -128-1), на яке може відповісти тільки відповідне абонентське обладнання (в даному випадку - SIM). Суть цього методу в тому, що існує величезна безліч подібних чисел і тому малоймовірно, що воно буде використано двічі.

Аутентифікація проводиться шляхом вимоги дати правильну відповідь на наступну головоломку: яку відповідь SRES абонент може вивести з надійшов RAND, застосовуючи алгоритм A3 з особистим (секретним) ключем Ki (рис.2.2).

Відповідь, який називається SRES (Signed RESult - підписаний результат), отримують в формі підсумку обчислення, що включає секретний параметр, що належить даному користувачеві, який називається Ki (рис. 1). Секретність Ki є наріжним каменем, покладеним в основу всіх механізмів безпеки - свій власний Ki не може знати навіть абонент. Алгоритм, що описує порядок обчислення, називається алгоритмом A3. Як правило, такий алгоритм зберігається в секреті (зайві запобіжні заходи ніколи не завадять!).

Для того, щоб досягти необхідного рівня безпеки, алгоритм A3 має бути односпрямованою функцією, як її називають експерти-кріптографи. Це означає, що обчислення SRES при відомих Ki і RAND має бути простим, а зворотну дію - обчислення Ki при відомих RAND і SRES - має бути максимально ускладнено. Безумовно, саме це і визначає в кінцевому підсумку рівень безпеки. Значення, що обчислюється за алгоритмом A3, повинно мати довжину 32 біта. Ki може мати будь-який формат і довжину.

Криптографічні методи дають можливість за допомогою відносно простих засобів домогтися високого рівня безпеки. У GSM використовуються єдині методи для захисту всіх даних, будь то для користувача інформація, передача сигналів, пов'язаних з користувачем (наприклад, повідомлень, в яких містяться номери викликаються телефонів), або навіть передача системних сигналів (наприклад, повідомлень, що містять результати радіовимірювань для підготовки до передачі). Необхідно усвідомлювати різницю тільки між двома випадками: який зв'язок виявляється захищеним (тоді всю інформацію можна відправляти в зашифрованому вигляді), який зв'язок є незахищеним (тоді вся інформація відправляється у вигляді незашифрованної цифрової послідовності).



 Рис. 2.3. Шифрування і розшифрування

Алгоритм А5 виводить послідовність шифрування из 114 біт для кожного пакету окремо, з урахуванням номера кадру і шифрувального ключа Кс.

Як шифрування, так і розшифровка виконуються із застосуванням операції «виключне або» до 114 «кодованим» бітам радіопакет і 114-бітової послідовності шифрування, що генерується спеціальним алгоритмом, який називається А5. Для того щоб отримати послідовність шифрування для кожного пакета, алгоритм А5 виконує обчислення, використовуючи два введення: одним з них є номер кадру, а іншим є ключ (який називається Кс), відомий тільки мобільній станції і мережі (рис. 2.3), В обох напрямках з'єднання використовуються дві різні послідовності: в кожному пакеті одна послідовність використовується для шифрування в мобільної станції і для розшифровки на BTS, в той час як інша послідовність використовується для шифрування в BTS і розшифровки в мобільній станції.

Номер кадру змінюється від пакета до пакету для всіх типів радіоканалів. Ключ Кс контролюється засобами передачі сигналів і змінюється, як правило, при кожному повідомленні. Цей ключ не оприлюднюється, але оскільки він часто змінюється, то не потребує таких сильних засобах захисту, як ключ Ki; наприклад, Кс можна вільно прочитати в SIM.

Алгоритм А5 необхідно встановлювати на міжнародному рівні, оскільки для забезпечення MS-роумінгу він повинен бути реалізований в рамках кожної базової станції (так само як і в будь-якому мобільному обладнанні). На даний момент один-єдиний алгоритм А5 встановлений для використання у всіх країнах. В даний час базові станції можуть підтримувати три основні варіанти алгоритму А5: А5 / 1 - найбільш стійкий алгоритм, який застосовується в більшості країн; А5 / 2 - менш стійкий алгоритм, впроваджуваний в країнах, в яких використання сильної криптографії небажано; А5 / 3 - відсутня шифрування. В Україні застосовується алгоритм А5 / 1. З міркувань безпеки його опис не публікується. Цей алгоритм є власністю організації GSM MoU. Проте, його зовнішні специфікації оприлюднені, і його можна представити як «чорний ящик», який приймає параметр довжиною 22 біта і параметр довжиною 64 біта для того, щоб створювати послідовності довжиною 114 бітів. Як і у випадку з алгоритмом аутентифікації A3, рівень захисту, пропонованої алгоритмом А5, визначається складністю зворотного обчислення, тобто обчислення Кс при відомих двох 114-бітових послідовностях шифрування і номера кадру.

Ключ Кс до початку шифрування повинен бути узгоджений мобільною станцією і мережею. Особливість стандарту GSM полягає в тому, що ключ Кс обчислюється до початку шифрування під час процесу аутентифікації. Потім Кс вводиться в незалежну пам'ять всередині SIM з тим, щоб він зберігався там навіть після закінчення сеансу зв'язку. Цей ключ також зберігається в мережі і використовується для шифрування.

 Всякий раз, коли будь-яка мобільна станція проходить процес аутентифікації, дана мобільна станція і мережа також обчислюють ключ шифрування Кс, використовуючи алгоритм А8 з тими ж самими вступними даними RAND і Ki, які використовуються для обчислення SRES за допомогою алгоритму A3.

Алгоритм А8 використовується для обчислення Кс з RAND і Ki (рис. 3). Фактично, алгоритми A3 і А8 можна було б реалізувати у формі одного-єдиного обчислення. Наприклад, у вигляді єдиного алгоритму, вихідні дані якого складаються з 96 біт: 32 біта для утворення SRES і 64 біта для утворення Кс.

Слід також зазначити, що довжина значної частини ключа Кс, видана алгоритмом А8, встановлюється групою підписів GSM MoU і може бути менше 64 бітів. В цьому випадку значущі біти доповнюються нулями для того, щоб в цьому форматі завжди були використані всі 64 біта.

Шифрування виявляється досить ефективним для захисту конфіденційності, але для захисту кожного окремо взятого обміну інформацією по радіоканалу не може використовуватися. Шифрування за допомогою Кс застосовується тільки в тих випадках, коли мережі відома особистість абонента, з яким йде розмова. Зрозуміло, що шифрування не може застосовуватися для загальних каналів, таких як ВССН, який приймається одночасно всіма мобільними станціями в даній стільникового осередку і в сусідніх стільникових осередках (інакше кажучи, воно може застосовуватися з використанням ключа, відомого всім мобільним станціям, що абсолютно позбавляє його сенсу як механізм безпеки). При переміщенні мобільної станції на будь-який спеціальний канал деякий час відбувається «початкове завантаження», протягом якого мережа ще не знає особистість абонента, скажімо, Володимира, і, отже, шифрування його повідомлення неможливо. Тому весь обмін сигнальними повідомленнями, що несе відомості про особу невизначеного абонента, повинен відбуватися в незашифрованому вигляді. Будь-яка третя сторона на даній стадії може підслухати інформацію про цю особистість. Вважається, що це обмежує права Володимира на секретність, тому в GSM введена спеціальна функція, що дозволяє забезпечити такого роду конфіденційність

Захист також забезпечується шляхом використання ідентифікаційного псевдоніма, або TMSI (Тимчасовий ідентифікатор мобільного абонента), яке використовується замість ідентифікатора абонента IMSI (Міжнародний ідентифікатор мобільного абонента) в тих випадках, коли це можливо. Цей псевдонім повинен бути узгоджений заздалегідь між мобільною станцією і мережею.

Особливо варто відзначити, що в наземному каналі передачі дані передаються по проводах в незашифрованому вигляді, і перехоплення інформації йде саме з них.

 2.3. Функції gsm каналів, які використовуються системами безпеки

 Досить сильно поширений на ринку систем безпеки в нашій країні тип сигналізацій використовує функцію SMS повідомлень. Така популярність обумовлюється низькою вартістю (самої сигналізації так і абонентської плати) та простотою використання даних GSM-сигналізацій. У професійних охоронних системах даний тип передачі сповіщень використовується в основному як сервісний канал. Оповіщення про надзвичайну ситуацію або про проникнення на об'єкт є обов'язковим атрибутом систем охорони і з точки зору технічної реалізації може бути виконано в такій формі як попередження голосом (дзвінком на телефон), DTMF (Dual Tone Multi-Frequency - термін для позначення тонального набору) кодом , в будь-якому цифровому вигляді, а також передачею SMS повідомлення власнику.

Для передачі повідомлень по засобом SMS повідомлень використовується найвідоміший GSM-сервіс мобільних операторів. І одночасно найпростіший в реалізації метод. GSM модеми з SMS-передавачем мають доступну ціну, в той же час прості в налаштуванні, а пультовим приймальним пристроєм може бути будь-який стільниковий телефон.

SMS (англ. Short Message Service - служба коротких повідомлень) - система, що дозволяє надсилати та отримувати текстові повідомлення у вигляді тексту за допомогою мобільного телефону. Текст може складатися з алфавітно-цифрових символів. Максимальний розмір повідомлення в стандарті GSM - 140 байт. Таким чином, при використанні 7-бітної кодування (латинський алфавіт і цифри) можна відправляти повідомлення довжиною до 160 символів. При використанні 8-бітного кодування (німецька, французька мова) можна відправляти повідомлення довжиною до 140 символів. Для підтримки інших національних алфавітів (китайського, арабського, російського і ін.) Використовується 2-байтне кодування UTF-16 (Unicode). Таким чином, SMS-повідомлення, написане кирилицею, не може перевищувати 70 знаків. Що вельми обмежує використання даного сервісу в охоронному обладнання.

У стандарті також передбачена можливість відправляти сегментовані повідомлення. У таких повідомлення в заголовку призначених для користувача даних (UDH) поміщається інформація про номер сегмента повідомлення та загальну кількість сегментів. Цю можливість підтримують не всі GSM-модеми, а ті, які підтримують, найчастіше накладають обмеження на кількість сегментів в повідомленні (3 або 5). Модем, який не підтримує сегментування, відображає кожен сегмент як окреме повідомлення. Як правило, кожен сегмент тарифікується як окреме повідомлення

Технологія SMS підтримується основними стільниковими мережами (GSM, NMT, D-AMPS, CDMA). Також SMS-повідомлення на телефони можна відправляти з інтернету та інших мереж, використовуючи спеціальні програми, а також безпосередньо шлюзи мобільних операторів.

 У своїй роботі GSM-сигналізації, що використовують SMS повідомлення для передачі тривожних повідомлень повністю ідентичні своїм аналогам, які використовують інші канали передачі даних. В даних сигналізаціях використовуються всі ті ж GSM-модеми. На об'єкті встановлюється контрольна панель з GSM-модулем. Залежно від типу зв'язку з датчиками (провідні та безпровідні охоронні датчики) підключаються охоронно-пожежні датчики. У разі спрацювання одного з датчиків, на панель надходить сигнал. У свою чергу в разі замикання однієї з зон, контролер дає команду GSM-модему відправити SMS повідомлення по одному або декільком номерів з пам'яті. Широке поширення набули так звані дачні охоронні сигналізації. Даний тип GSM-сигналізацій майже завжди поєднує в собі охоронні функції та функції дистанційного керування виконавчими пристроями. У професійній охороні даний тип зв'язку застосовується обмежено, в основному як сервісний канал, наприклад для підтвердження взяття об'єкта під охорону або контроль напруги мережі на об'єкті. Так само даний канал використовується як останній резервний канал в професійних охоронних системах.

Слабке місце даних охоронних систем всім добре відомо: SMS-повідомлення можуть затримуватися в SMS-сервері на невизначений час, а іноді просто губляться. Оскільки даний канал зв'язку не є пріоритетним. У разі завантаженості GSM каналу SMS повідомлення відправляються в останню чергу (чого не скажеш про голосові дзвінки). Невизначеність часу доставки SMS повідомлень роблять цей метод неприпустимим для професійної охорони.

Таблиця 2.1. Підтримка способів передачі сповіщень на ПЦС



 Voice (мовний) канал умовно поділяється на DTMF сигнал і мовне оповіщення. Даний канал дуже популярний серед пультових охоронних систем. У даного каналу GSM мережі є свої плюси і мінуси. З плюсів можна виділити простоту переходу з провідної охоронно-пожежної сигналізації на GSM-сигналізацію. Мінуси - це забивання каналу в разі несправності або поганого сигналу.

Voice канал - cамий поширений канал передачі даних в охоронних системах,який використовує GSM технології передачі даних. Voice канал - це голосовий тракт,що використовує мовне оповіщення (зазвичай в приватних охоронних системах) і DTMF-код (обладнання для пультів централізованого спостереження).

Про мовному оповіщенні в разі тривоги GSM-сигналізація дзвонить на телефон і промовляє заздалегідь записане повідомлення.

З DTMF трохи складніше. У DTMF при натисканні на клавішу кнопкового телефону лунає звук (тон), який є комбінацією двох тонів, високо- і низькочастотного.

Система сигналів DTMF включає вісім тонів, які були спеціально підібрані таким чином, щоб передаватися через телефонну мережу без загасання і з мінімальним впливом один на одного. Оскільки ці звукові сигнали потрапляють в частотний діапазон людського голосу, були додатково введені заходи для того, щоб голос не сприймався як набір. Одна з таких заходів - розподіл тонів на дві групи, високо- і низькочастотну.

Таблиця 2.2. Можливості, які подаються різними системами охорони.



 Зазвичай в GSM-сигналізації для пультів централізованого спостереження (ПЦС) використовуються стандартні формати, наприклад протокол Contact ID. На даний момент DTMF - найпоширеніший канал передачі даних, оскільки формати даних, принцип передачі, приймальне обладнання - повністю запозичене у проводового моніторингу. Наприклад, якщо охоронне підприємство вже має станцію централізованого моніторингу, то застосування GSM-сигналізацій не викликає зайвих витрат, тому що не потрібно замінювати обладнання на станції моніторингу. Використання DTMF форматів висуває додаткові вимоги до опрацювання звукового тракту GSM-модему. Аналого-цифрові перетворення тягнуть за собою спотворення при передачі сигналу. Через це можуть відбуватися збої при прийомі звітів від об'єктового обладнання. Дана проблема досить часто зустрічається у вітчизняного обладнання. І хоча сигнал не згубиться в мережі (більшість систем контролюють передачу даних, запитуючи, чи потрібно приймати), але значно збільшиться час проходження сигналу. Причому збільшення часу проходження сигналу може бути фатальним. Уявіть собі ситуацію, коли на об'єкт встановлено обладнання використовує передачу даних в форматі DTMF кодів. Через несправність обладнання або із-за поганої якості сигналу, об'єктовий прилад не зможе передати повідомлення на пульт. І, як наслідок, не отримає підтвердження про прийом. Не отримавши повідомлення про прийом прилад почне повторний набір, зі спробою передати повідомлення. Але в підсумку, не отримавши нічого, починається цикл дозвонів. Цей цикл повністю займе весь канал, що не дозволить передати повідомлення іншим об'єктовим приладів, тобто буде втрачено зв'язок з об'єктами. Не буде повідомлень про тривогу, що не буде повідомлень про постановку і зняття з охорони і т.д. І як наслідок повністю неробочий пульт централізованого спостереження.

CLIP (Calling Line Identification Presentation).

Даний метод заснований на сервісі оператора мобільного зв'язку по наданню інформації про номер абонента, що здійснює дзвінок. Принцип систем, що використовують CLIP, дуже простий. Об'єктовий ППКОП в разі системного події здійснює дзвінок по мережі стільникового зв'язку на приймальний пристрій, в якості якого може виступати GSM-модем або звичайний мобільний телефон. Приймальний пристрій зчитує номер абонента і відхиляє виклик. Сам факт дзвінка від відомого в системі абонента і є підставою для реєстрації тривожної події. Вигода методу очевидно - відсутня плата за вихідний дзвінок, адже ніякого з'єднання не відбувається. Однак інформативність такого повідомлення дуже мала. Правда, цей спосіб можна видозмінити для підвищення інформативності. Наприклад, встановити на ПЦС кілька GSM-модемів Передавальний пристрій програмують таким чином, щоб по одній групі подій модем робив виклик на перший модем (тривоги), по іншій групі - на другий і т.д. Слід зазначити, що даний спосіб не знайшов істотного поширення через малу інформативность.

 GSM DATA / CSD (Circuit Switch Data).

 Цифровий канал передачі даних на швидкості 9,6 кбіт / с. Цей метод характеризується практично 100% -ною вірогідністю доставки повідомлення. Час встановлення з'єднання близько 20 с. Тарифікація CSD похвилинна, як і для голосового каналу GSM. На відміну від передачі повідомлення в стандартному форматі Contact ID в голосовому каналі, протокол передачі в CSD не стандартизований (хоча може бути максимально наближений до CID).

 Це не дозволяє використовувати передавачі одного виробника в системі іншого виробника (звичайно, якщо вони не домовилися і не вжили спеціальних заходів по сполученню своїх систем).

Можлива установка в "прозорому" (transparent) і "непрозорому" (non-transperent) режимах. Відмітна особливість передачі даних з використанням "непрозорого" режиму- велика перешкодозахищеність, що досягається за рахунок введення алгоритму корекції помилок, а також наявності підтвердження успішної (без спотворень) доставки інформації, що передається. Таким чином, використання "непрозорого" CSD-з'єднання представляється кращим при низькому співвідношенні сигнал / шум. Однак тривалість часу встановлення з'єднання в "непрозорому" режимі більше, ніж в "прозорому". У режимі CSD також реалізована процедура підтвердження прийнятих повідомлень на ПЦС.

 TCP / IP GPRS (General Packet Radio Service).

 Як відомо, технологія пакетної передачі GPRS використовує в якості механізму доставки пакетів даних протоколи TCP / IP, в разі застосування яких кожному з пристроїв мережі присвоюється унікальний IP-адресу. Існує два види IP-адрес: статичні і динамічні. Статичні IP-адреси можуть надаватися або Інтернет-провайдерами, або операторами стільникових мереж.

Динамічні IP-адреси видає оператор при приєднанні до мережі GPRS і тільки на час сеансу зв'язку. Якщо з яких-небудь причин сеанс перервався, то при повторному приєднанні пристрій, що не має статичного IP-адреси, отримає новий динамічний, відмінний від попереднього. Необхідно згадати той факт, що якщо пристрій, в тому числі модем GSM / GPRS, авторизувалось в мережі і отримало динамічний IP-адресу, то для підтримки віртуального GPRS-каналу в активному стані потрібно через певні часові інтервали передавати сигнальні пакети на будь-який відомий IP- адрес, інакше оператор роз'єднає з'єднання з мережею. Можливі різні варіанти виділення IP-адрес ЦПО та концентраторів мереж лічильників. Найбільш часто зустрічається варіант - наявність у ЦПО статичного IP-адреси, а у абонентів - динамічних. Причому статичний IP-адресу виділяє ЦПО НЕ стільниковий оператор, а Інтернет-провайдер при підключенні ЦПО до Інтернету по виділеному каналу доступу (утвореному за допомогою технологій ЛВС, ADSL або ін.).

 При такій організації системи можливі два сценарії встановлення з'єднання між пристроями з метою передачі даних. Якщо тим пристроєм,що ініціював з'єднання є концентратор, він організовує GPRS-сеанс з інфраструктурою стільникового оператора, отримує від нього динамічну IP-адресу і встановлює TCP / IP-з'єднання з ЦПО (якщо "знає" його статичну IP-адресу). Останній (ЦПО) повинен бути налаштований на прийом (і обробку) запитів на з'єднання по виділеному каналу доступу в Інтернет. Під час отримання запиту на з'єднання від концентратора його динамічна IP-адреса стане "відома" ЦПО (в IP-заголовку пакета міститься інформація про адресу відправника), що зробить можливим двосторонній обмін інформацією Якщо ж ініціатором зв'язку є ЦПО, то він додзвонюється до віддаленого модему по голосовому каналу GSM або надсилає SMS-повідомлення на його номер. Концентратор сприймає вхідний дзвінок (або яке надійшло SMS-повідомлення) з відомого номера як команду на встановлення з'єднання з ЦПО і далі діє так, як було описано раніше. Мінімальною вимогою при організації з'єднання з ЦПО є "знання" концентратором статичної IP-адреси ЦПО. Якщо ж концентратор не «знає» цю адресу, то його можна повідомити концентратору по голосовому каналу GSM або за допомогою служби SMS.

 При необхідності організувати зв'язок з концентратором, що має статичну IP-адресу, ЦПО звертається до нього за цією адресою, встановлюючи GPRS-з'єднання. Для цього модем GSM / GPRS концентратора повинен бути налаштований на прийом (і обробку) запитів на з'єднання по каналу TCP / IP. Такий спосіб організації каналу передачі даних можливий, однак на практиці майже не зустрічається через складність отримання статичних IP-адрес у стільникових операторів для всіх віддалених пристроїв системи. Актуальний і такий варіант: концентратори і ЦПО мають динамічні IP-адреси. Це можливо, коли ЦПО не обладнано виділеним каналом доступу в Інтернет, але розташований в зоні дії одного з операторів стільникового зв'язку. У цьому випадку вже не важливо хто є ініціатором зв'язку - концентратор або ЦПО, дії по реалізації каналу передачі даних завжди будуть одні і ті ж.

 Ініціювавший зв'язок пристрій (наприклад, ЦПО) організовує GPRS-сеанс з інфраструктурою стільникового оператора і отримує від нього динамічну IP-адресу. Потім він повідомляє (наприклад, за допомогою служби SMS) отриману адресу іншого пристрою (концентратора) і передає йому команду з'єднатися за цією адресою. Викликається пристрій, організувавший GPRS-сеанс і отримавши динамічну IP-адресу, встановлює TCP / IP-з'єднання із з пристроєм,що ініціював зв'язок.

2.4. Аналіз завадостійкості і перешкодозахищеності gsm каналу

Перешкоди в радіоканалі створюються як за рахунок спотворень сигналу при його поширенні, так і в результаті впливу зовнішніх джерел. Перший тип спотворень порівняно легко усунути, в той же час з перешкодами від зовнішніх джерел борються за допомогою розширення спектра сигналу, що передається. Теоретично, збільшення бази сигналу (твір ефективного значення тривалості сигналу і ефективного значення ширини його спектра) дозволяє зменшити перешкоду до як завгодно малого рівня.

 Основна складність при побудові GSM каналу пов'язана з неможливістю забезпечити безперервність GSM / GPRS-зв'язку з оператором через перебої в мережі, які призводять не лише до переривання передачі даних, але і до зависання модему. Практика показує, що жоден GSM-оператор на сьогоднішній день не забезпечує надання гарантованого GPRS-каналу зв'язку. У спробах реалізації безперервності підключення розробники змушені додатково оснащувати традиційні (прості) GSM-модеми додатковими пристроями - зовнішніми контролерами, сторожовими таймерами, які здійснюють перезавантаження модему при зависанні. На жаль, подібні рішення хоч і є зазвичай «економічними», але як і раніше не гарантують безперервного і безперебійного процесу передачі даних, а також ведуть до ускладнення системи в цілому і, як наслідок, до зниження її надійності.

Додатково до перерахованих методів, для підвищення завадостійкості РЕЗ, що використовують вузькосмугові сигнали, застосовують багаторазове дублювання фрагментів переданих повідомлень в частотній або тимчасовій області. Наприклад, модеми для передачі даних в короткохвильовому діапазоні частот використовують для одночасної передачі інформації до 50 несучих частот використовуються повільні скачки по частоті SFH (Slow Frequency Hopping) або інакше - повільна псевдовипадкова або програмна перебудова радіочастот (ППРЧ). Використання ППРЧ спільно з перешкодостійким кодуванням і перемежением дозволяє в умовах вузькосмугових перешкод в каналах з завмираннями підвищити стійкість перед перешкодами на прийомі на 9-11дБ, в той час, як без ППРЧ ця цифра коливається в межах 4-6дБ.

Перешкодостійкість, на думку цілого ряду фахівців в області радіо канальних пожежних і охоронних систем, визначається наступним:

- кількістю частотних діапазонів, в яких може працювати радіосистема;

- кількістю частотних каналів в кожному діапазоні;

- можливістю автоматичного вибору резервних каналів;

- наявністю автоматичного регулювання потужності випромінювання.

Відповідно до європейської класифікації існує три класи пожежних і охоронних дротових і радіо канальних систем, що відрізняються між собою, перш за все, за ступенем ризику технічно підготовленого злому (ЕМ 50131-1):

 - клас А: низький ступінь ризику - об'єкти приватного користування (заміські будинки, квартири);

 - клас В: середній ступінь ризику-об'єкти громадського користування (магазини, навчальні заклади);

 - клас С: висока ступінь ризику - об'єкти державної важливості (музеї, історичні пам'ятки).

 Уявімо собі типову ситуацію на об'єкті, що знаходиться під охороною радіосистеми. Час від часу пропадає зв'язок з тим чи іншим радіопристроєм. Швидше за все, причиною є не навмисне саботування роботи системи, а робота інших приладів і систем на обраному при установці системи каналі зв'язку (літері). Нагадаємо, що діапазон частот 433 і 868 МГц є неліцензованим, і його використовують не тільки пожежні та охоронні радіосистеми, а й побутові пристрої:

переносні радіостанції, іграшки, шлагбауми і т. д. В залежності від класу радіосистеми повинні реагувати по-різному:

 - клас А: індикація про тимчасову втрату зв'язку з радіопристроєм системи відсутня;

 - класи В і С: радіосистема зобов'язана максимально використовувати всі можливі способи доставки сигналу і тільки після цього передати сигнал "Тривога". Наприклад, сповіщувач, не отримавши квитанцію від приймально-контрольного приладу після передачі тестового сигналу (що можливо тільки в системі з двостороннім протоколом), негайно змінює частотний канал, потужність випромінювання, періодичність виходу в ефір і т. д. Якщо зв'язок не може бути відновлений навіть після всіх згаданих дій, то в даному випадку має місце навмисне саботування роботи системи.

Здатність радіолінії працювати в умовах впливу організованих перешкод називається перешкозахистом.

 Перешкозахист розділяється на два класи:

1) просторовий перешкозахист (за рахунок низького рівня бічних пелюсток прийомної антени, за якими діє перешкода, формування «нулів» діаграми спрямованості приймальної антени в напрямку на джерело перешкод);

2) сигнальний перешкозахист за рахунок широкосмугових методів модуляції.

Принцип придушення заснований на постановці вузькополосної перешкоди приймальному каналу GSM-пристрою. На сьогоднішній день заглушувачів GSM-пристроїв велика кількість і основне їх використання - заглушати мобільні телефони на нарадах, конференціях, бібліотеках, театрах і т.п. Однак це не заважає застосовувати їх і для негативних цілей. Їх застосування не залишиться не поміченим для операторів мобільного зв'язку.

Відомі кілька типів пристроїв, застосовуваних для глушіння супутникових охоронних систем:

1. Широкополосна глушилка. Постійно випромінює потужний шум на всіх робочих частотах GSM. Тим самим GSM-модуля перестає бачити як супутники GPS, передають поточні координати автомобіля, так і БС оператора GSM.

 2.Така,що перебирає частоти -- тип глушилок працює так само , як перший тип, відмінність в тому, що шумоподібна перешкода ставиться послідовно по всіх частотах каналу GSM, не дозволяючи GSM-модуля передавати сигнал. Розміром вона досить компактна і живиться від звичайних батарейок. Діє в радіусі 5-15 метрів.

 3. «Розумна» - це глушилка, яка видає себе за базову станцію оператора GSM. При її включенні, GSM-модуль буде працювати без збоїв і вважати, що все добре. Глушилка вимагає серйозного джерела живлення.

На сьогодні існує два способи боротьби з глушінням:

- визначення факту глушіння на стороні GSM-модуля. Якщо модуль бачить, що в ефірі на робочих частотах з'явився сигнал (шум), він намагається встигнути зробити оповіщення. Але це малоймовірно, адже відправити SMS або голосове повідомлення навряд чи вийде, тому що передавач вже заглушений.

- визначення факту глушіння ззовні. Для цього організовується постійна перевірка зв'язку між GSM-модулем і спеціально виділеним сервером -контроль каналу. Таким чином, на стороні сервера можна гарантовано визначити пропажу зв'язку з автомобілем. Що стосується пропажі GSM-сигналу, сервер сповіщає власника SMS-повідомленням, по e-mail, або дзвінком.

Для зниження глушіння сигналу потрібно:

- мати дублюючий канал для обміну важливою інформацією;

- використовувати періодичний тест з об'єкта;

- застосувати виносні антен.

2.5. Дослідження швидкості передачі даних і пропускної здатності gsm каналу.

 Максимальна швидкість передачі даних по одному голосовому каналу GSM (режим CSD) становить 9600 Кбіт / с, а багатоканальний режим HSCSD забезпечує передачу даних на швидкості 19 200 Кбіт / с і вище.

Таблиця 2.3. Перелік послуг і якість роботи додатків на різних швидкостях передачі



Таблиця 2.4. Характеристики поколінь GSM



До недоліків використання голосового каналу GSM можна віднести значну вартість пересилки кілобайта інформації і істотний негативний вплив (на економічні показники системи) часу організації сеансу зв'язку між модемами при передачі малих обсягів даних. Наприклад, час передачі 20 Кбіт інформації дорівнює приблизно 2 с, а час організації сеансу може варіюватися від 2 до 16 с, в залежності від режиму роботи модемів.

Максимально можлива швидкість обміну даними за допомогою технології GPRS теоретично може досягати 170 Кбіт / с.



Рис.2.4. Залежність пропускної здатності від схеми кодування.

В технології GPRS була запропонована нова структура пакету розміром 456 біт (чотири інформаційних блоки по 114 біт), яка забезпечує загальну швидкість передачі по каналу 22,8 кбіт / с

З метою підвищення гнучкості передачі і пропускної здатності в системі GPRS можуть використовуватися чотири схеми кодування даних: від CS1 до CS4. Для керування роботою радіолінії в режимі пакетної передачі розроблений спеціальний протокол RLC (Radio Link Control), який забезпечує її адаптивну настройку, програмну перебудову частоти і керування потужністю. Адаптація радіолінії включає вибір тієї чи іншої схеми кодування (CS1 - CS4) в залежності від виду переданої інформації, характеристик радіоканалу і рівня перешкод.

 Таким чином, в режимі GPRS кожному абоненту надається від 1 до 8 канальних інтервалів. Під час пакетної передачі ресурси ліній зв'язку «вгору» і «вниз» можуть виділятися незалежно один від одного, тобто в системі допускається реалізація асиметричного режиму передачі. Сьогодні при використанні схеми кодування CS2 швидкість передачі даних в GPRS-системі становить 115,2 (8х14,4) кбіт / с, однак теоретично вона може бути збільшена до 171,2 (8х21,4) кбіт / с - якщо застосувати схему кодування CS4 .

Проведені в жовтні 2008 року дослідження швидкості мобільного з'єднання показали, що реально середня швидкість становить вхідного з'єднання 130 Кбіт / c, що виходить - 57 кбіт / c. Жоден з операторів мобільного Інтернету не показав максимально можливу для використовуваного їм стандарту швидкість (474 ​​Кбіт / c для EDGE у GSM).

Окремо варто згадати, що швидкість передачі значно зростає при використанні технології EDGE. EDGE (англ. Enhanced Data rates for GSM Evolution) - цифрова технологія для мобільного зв'язку, яка функціонує як надбудова над 2G і 2.5G (GPRS) -Мережі. Для підтримки EDGE в мережі GSM потрібні певні модифікації і удосконалення. На основі EDGE можуть працювати: ECSD - прискорений доступ в Інтернет по каналу CSD, EHSCSD - по каналу HSCSD, і EGPRS - по каналу GPRS. EDGE був вперше представлений в 2003 році в Північній Америці. Незважаючи на те, що EDGE не вимагає апаратних змін в NSS-частини мережі GSM, модернізації повинна бути піддана підсистема базових станцій (BSS). Необхідно встановити трансивери, що підтримують EDGE (8PSK модуляцію) і оновити програмне забезпечення. Також потрібні телефони, що забезпечують апаратну і програмну підтримку модуляції і кодових схем, які використовуються в EDGE.

3. Дослідження технічних характеристик систем безпеки, що використовують gsm канали.

Охоронні системи на основі GSM можна використовувати, як для особистих цілей, так і в комплексних централізованих системах охорони і моніторингу. Дуже вигідно, а іноді єдино прийнятно, використання GSM сигналізації на об'єктах, де утруднена прокладка кабельних і телефонних мереж.

GSM-сигналізація підвищує захищеність об'єкта власності завдяки наступним факторам:

- факт наявності сигналізації змусить недосвідчених злочинців відмовитися від своїх злочинних намірів;

- оперативна передача тривожного повідомлення на телефон власника або на ПЦС, а так само спрацьовування сирени, приведуть, в кінцевому рахунку, до прибуття на місце групи швидкого реагування або наряду міліції, що в свою чергу призведе до затримання злочинців.

Перша, і дуже важлива умова: сигналізація повинна бути вандалостійкою, тобто перебувати в металевому боксі, де встановлені всі елементи, в т. ч. - GSM-термінал, колодки підключення шлейфів, блок живлення. Це необхідно для виконання головних її функцій - передачі тривожного повідомлення і включення інших пристроїв.

Друга - прилад повинен мати не менше 4 роз'ємів для підключення різних датчиків. Бажано, щоб ці зони були програмованими - наприклад, до першого роз'єму - ланцюжок датчиків руху, до другого - ланцюжок димних датчиків, до третього - геркон на вхідних дверях, до четвертого - ланцюжок датчиків удару. Також не завадить 2 виходи на виконавчі пристрої (наприклад, світлову і звукову сигналізацію).

Третя - особливу увагу необхідно приділити наявності та якості вбудованого джерела живлення. Джерело безперебійного живлення і батарея повинні забезпечувати надійну роботу централі і підключених до неї датчиків при відключенні живлення протягом як мінімум доби. Блок живлення повинен захищати акумуляторну батарею від глибокого розряду і витримувати коротке замикання виходів живлення 12 В.

Четверта - бажано, щоб була виносна індикація, яка дозволяє візуально контролювати стан приладу. Це важливо при використанні електронних ключів типу Touch Memory, радіобрелків і карт для дистанційної постановки і зняття приладу з охорони.

П'ята - добре, щоб система могла в одному повідомленні повністю описувати стан всієї системи: тривоги із зазначенням зони, стану системи, описувати, які реле включені, скільки залишилося заряду в батареї, який стан телефонної лінії (якщо вона є). Є і опціональні параметри - наприклад, в залежності від свого «інтелекту», системи GSM-охорони можуть не тільки повідомляти власника про проблеми, а й самостійно реагувати на такі подразники. Зловмисники можуть і блокувати стільникову мережу в окрузі за допомогою банальної стільникової «глушилки», тому важливо, щоб у відповідь, скажімо, на вторгнення система не тупо перебирала номера для повідомлення настільки «радісною» новини, а відразу відкривала клітки з собаками-охоронцями, запалювала світло, включала сирену або пускала сльозогінний газ.

Шоста - дуже важливо, щоб сигналізація вміла контролювати наявність або відсутність сигналу базової станції. Практично для всіх моделей GSM-сигналізацій застосування зловмисником пристроїв придушення сигналу або створення перешкод є нерозв'язною проблемою. Система повинна подавати сигнал попередньої тривоги власнику будівлі при погіршенні якості сигналу від базової станції. Важливо, якщо GSM панель передає повідомлення одночасно декільком користувачами і пультів централізованого спостереження. Повідомлення для ПЦС повинні передаватися в зашифрованому вигляді (це підвищує надійність охоронного комплексу). Повідомлення для користувача повинні легко читатися і бути максимально інформативними. Добре, коли в одному повідомленні повністю описується стан всієї системи. Тривога із зазначенням зони, стан централі, які реле включені, чи є мережа 220, заряд АКБ, стан телефонної лінії (якщо вона є).

З точки зору підтримки стабільного радіозв'язку необхідне використання таких елементів як виносні антени. Існують три ситуації, в яких стаціонарні спрямовані пасивні антени можуть допомогти:

- нестійкий зв'язок на кордоні зони покриття з граничною віддаленостю від найближчої базової станції (БС)

- робота всередині зони покриття, але в місцях відсутності сигналу (складки рельєфу, екранування великими природними і штучними спорудами)

- зв'язок всередині приміщення з високим ступенем ослаблення сигналу (підвали та напівпідвали, металеві споруди, будівлі, обшиті металом і т.д.).

Реальне розширення зони покриття за рахунок застосування виносної антени може бути здійснено, але вельми в скромних межах. Причому це збільшення сильно залежить від використовуваного стандарту.

Досить сильний ефект дає використання GSM-репітерів, але через високу вартість застосовувати їх раціонально на великих об'єктах.

Серйозну проблему становить перевантаженість ліній зв'язку в великі свята. Рішенням проблеми є установка об'єктового приладу з sim-картами двох різних стільникових операторів зв'язку.

Оптимальним для GSМ-сигналізацій є комбінування різних функцій (SMS, Voice). Також ефективним є використання GSM як дублюючого або додаткового каналу проводовим і іншою радіоканальною системою передачі сповіщення. З точки зору пропускної здатності каналу виправдане використання технології EDGE. Правда, ця технологія (як і 3G) не отримала ще широкого розповсюдження.

4. Охорона праці

4.1 Аналіз небезпечних і шкідливих факторів при виробництві

У цій частині дипломного проекту розглянемо умови виготовлення та умови експлуатації розробленого пристрою з урахуванням організації безпеки праці.

Категорії тяжкості виконуваних робіт при виготовленні та експлуатації виробу встановлюються відповідно до ГОСТ 12.1.005-88. Умови виготовлення та експлуатації пристрою відносяться до 1-ої категорії і - легкі фізичні навантаження. Відповідно до цього ж ГОСТом встановлюються параметри температури навколишнього повітря, відносної вологості, щільності і швидкості руху повітряного потоку на робочому місці.

Відповідно до ГОСТ 12.0.003-74 "ССБТ. Небезпечні і шкідливі виробничі фактори. Класифікація »поділяються за природою дії на чотири групи:

* фізичні;
* хімічні;
* біологічні;
* психофізіологічні.

Кожна з яких поділяється на підгрупи.

До фізичних факторів належать рухомі машини та механізми; невідповідність нормам мікроклімату в робочій зоні; неприпустимі рівні шуму, вібрації, ультразвуку, електромагнітних та іонізуючих випромінювання; електричний струм; недоліки освітлення та ін.

До хімічних факторів відносяться шкідливі для організму людини речовини: загальнотоксичні, дратівливі, канцерогенні (викликають розвиток пухлин), сенсибілізуючі (що викликають алергічні захворювання), мутагенні. У цю групу входять шкідливі пари бензолу, толуолу, окису вуглецю, сірчистого газу, окису азоту, хлору, а також аерозолі свинцю, сполуки хрому, токсичного пилу, що утворюються при обробці різанням свинцевих бронз і латуней, шаруватих пластиків, кераміки, напівпровідникових матеріалів. Крім того, до них відносяться агресивні рідини, які можуть викликати гострі та хронічні захворювання шкіри.

До біологічних факторів відносяться мікроорганізми (бактерії, віруси, спірохети) і макроорганізми (рослини і тварини).

До психофізіологічних факторів - фізичні та нервно-психічні перевантаження: розумові перенапруження, монотонність праці та емоційні перевантаження.

Найбільш небезпечними виробничими факторами є шкідливі речовини. Згідно ГОСТ 12.1.007-76 "ССБТ. Шкідливі речовини, класифікація і загальні вимоги безпеки "[20].

За ступенем впливу на організм шкідливі речовини підрозділяються на чотири класи небезпеки:

* надзвичайно небезпечні;
* високонебезпечні;
* помірно небезпечні;
* малонебезпечні.

У результаті дії небезпечних і шкідливих виробничих факторів, шкідливих речовин можуть мати місце нещасні випадки і професійні захворювання.

Аналіз причин нещасних випадків дозволяє згрупувати їх умовно на технічні, організаційні, санітарно-гігієнічні, психофізіологічні, економічні та соціально-психологічні.

Для підприємств радіоелектронної промисловості характерні наступні професійні захворювання:

* отруєння;
* пневмоконіози;
* бериліоз;
* гострі та хронічні захворювання шкіри;
* катаракта;
* електроофтальмія;
* кон'юнктивіти і ін

Відповідно до ГОСТ 12.0.002-80 безпеку виробничих процесів забезпечується вибором технологічного процесу.

ТП виготовлення блоку складається з різних технологічних операцій: виготовлення деталей, складання їх у виріб, наладки блоку. Розглянемо перераховані вище технологічні операції. При механічній обробці матеріалів виникає ряд небезпечних і шкідливих виробничих факторів:

* рухомі частини виробничого обладнання;
* ріжучі інструменти;
* висока температура поверхні оброблюваної деталі;
* стружка, пил, шум, вібрація.

Сучасна технологія виготовлення ПП складається з великої кількості операцій. При виготовленні ДП можуть виникнути такі небезпеки:

* ураження електричним струмом;
* термоопіки та хімічні опіки;
* ураження шкірних покривів;
* отруєння;
* шум, вібрація;
* світлові впливу газорозрядних ламп.

Більшість речовин і матеріалів, що застосовуються при виготовленні ДП, є шкідливими і становлять небезпеку для здоров'я і життя людини. Шкідливі речовини та їх пари можуть проникати в організм людини через органи дихання, шкіру, травний тракт.

Електричні з'єднання виробляються паянням. ТП включає в себе видалення ізоляції і лудіння. При виконанні пайки на робітника можуть впливати наступні шкідливі і небезпечні фактори:

* запиленість і загазованість повітря робочої зони;
* попадання розплавленого припою на шкірний покрив;
* наявність нагріваються елементів, дотик до яких викликає опіки.

Для виявлення порушення норм з охорони праці та запобігання травматизму важливе значення має єдиний для всіх галузей народного господарства порядок розслідування та обліку нещасних випадків на виробництві "Положенням про розслідування та облік нещасних випадків на виробництві".

4.2 Заходи з охорони праці

На основі описаних в розділі 5.1 небезпечних і шкідливих виробничих факторів розроблено ряд заходів щодо забезпечення охорони праці.

Відповідно до ГОСТ 12.1.030-81, для захисту людей від ураження електричним струмом при дотику до металевих неструмоведучих частин, які можуть опинитися під напругою в результаті пошкодження ізоляції, передбачаються наступні заходи:

* захисне заземлення;
* занулення;
* мала напруга;
* захисне відключення:
* ізоляція струмоведучих частин;
* огороджувальні пристрої;
* попереджувальна сигналізація;
* блокування;
* запобіжні пристосування та ін

Відповідно до ГОСТ 12.2.003-74 при роботі на фрезерних і свердлильних верстатах, небезпечні зони огороджуються. Верстати оснащуються екранами, які захищають робітників від відлітаючої стружки і осколків інструменту, що зламався, або від бризок змащувально-охолоджувальної рідини.

Для зниження виробничого шуму редуктори поміщають в звукоізолюючі кожухи, зубчасті колеса поміщають в масляні ванни, застосовують акустичні екрани, що відокремлюють одне робоче місце від іншого, засоби індивідуального захисту - навушники.

При виготовленні друкованих плат щоб уникнути травм і профзахворювань робота з шкідливими речовинами виробляється з використанням фільтруючих засобів індивідуального захисту органів дихання, до яких відносяться універсальні респіратори і протигази. Для захисту рук в якості засобів індивідуального захисту застосовуються рукавиці та рукавички з різноманітних матеріалів, а також захисні мазі, пасти і т.д. Для захисту очей застосовують окуляри.

Для зниження шкідливих факторів при нанесенні захисних покриттів і пайці, основними методами захисту є загальна вентиляція з місцевими відсмоктувачами і індивідуальні засоби захисту.

Кількість необхідного повітря, що подається в залежності від кількості шкідливих речовин, що виділяються, визначається за формулою (5.1):

  (4.1)

де L - кількість повітря, що видаляється з робочої або обслуговуючою зони приміщення місцевими відсмоктувачами, загальнообмінною вентиляцією і на технологічні або інші потреби, м/годин;

Z - кількість шкідливий речовин, що надходять у повітря приміщення, мг / год;

З м - концентрація шкідливих речовин у повітрі, що видаляється з робочої зони місцевими відсмоктувачами на технологічні або інші потреби, мг/м3;

C ух - концентрація шкідливих речовин у повітрі, що видаляється з приміщення, мг/м3 ;

C n - кількість шкідливих речовин у повітрі, що подається в приміщення, мг/м3.

У якості місцевих відсмоктувачів при пайці застосовуються шарнірно-телескопічні відсмоктувачі прямокутної форми, які встановлюються у вертикальній площині столу. Для ручної пайки використовується монтажний стіл.

Кількість відсмоктується повітря для прямокутних отворів з гострими крайками (м  / С) визначається за формулою:

  (4.2)

де S - площа отвору всмоктування, м3;

Е - велика сторона прямокутного отвору всмоктування, м (Е = 0,14÷0,28 м);

Х - відстань від площини отвору всмоктування до аналізованої зони пайки, м (Х=0,1÷0,3 м);

V x - швидкість руху повітря в зоні пайки, м/с.

Менша сторона прямокутного отвору всмоктування визначається з оптимального співвідношення:

  (4.3)

 

Приймаю: Z = 50 мг/год; См = 1 мг/м3, Сух = 2 мг/м3, ЗП = 0, тоді



За результатами розрахунку можна зробити висновок, що для забезпечення хорошої вентиляції приміщення при виробництві даного блоку необхідно подавати в робоче приміщення 39,4 м3/год чистого повітря.

Для забезпечення витяжної вентиляції будемо використовувати відцентровий пиловий вентилятор В-ЦП-7-40 № 6 з клиноремінним приводом, який буде встановлений на даху будівлі.

Даний вентилятор має такі характеристики:

* продуктивність - 5000 м3/год;
* частота обертання - 1755 об/хв;
* тип електродвигуна - 4А132 S 4;
* потужність електродвигуна - 7,5 кВт;
* частота обертання електродвигуна - 1455 об/хв.

Правильно обрана система освітлення має велике значення у зниженні виробничого травматизму, створює нормальні умови для роботи органів зору, підвищує працездатність. Приміщення має чотири вікна висотою 2 м, і шириною 2 м, розташованих на одній стіні. Згідно СНИП П-4-79, коефіцієнт природної освітленості (КПО) в нашому випадку при бічному освітленні складає *е=1,5%* .

При бічному освітленні КПО можна оцінити за формулою

     (4.4)

 де SП - площа підлоги приміщення, м2;

SО - площа світлових прорізів, м2;

КЗ - коефіцієнт запасу (приймається в межах від 1.2. до 2.0 залежно від можливого забруднення світлових прорізів кіптявою);

 - світлова характеристика вікон;

КЗД - коефіцієнт, що враховує підвищення коефіцієнта завдяки світлу, відбитому від поверхні приміщення та підстилаючого шару, прилеглого до будівлі;

 - загальний коефіцієнт світлопропускання, що визначається за формулою

  (4.5)

де τ1- коефіцієнт світлопропускання матеріалу (для різних типів скла приймається в межах від 0.65 до 0.9);

τ2 - коефіцієнт, що враховує втрати світла в межах вікна (залежно від виду палітурки приймається в межах від 0.5 до 0.9);

τ3 - коефіцієнт, що враховує втрати світла в несучих конструкціях (від 0.8 до 0.9);

τ4 - коефіцієнт, що враховує втрати світла в сонцезахисних пристроях (при їх відсутності τ4=1 , за їх наявності τ4 приймається від 0.6 до 0.9).

 Площа світлових прорізів становить SО=16 м2, площа підлог приміщення становить SП=100 м2. Для складальних цехів коефіцієнт запасу приймається КЗ=1,2. Виходячи із співвідношення розмірів приміщення і вікон, світлова характеристика вікон . Коефіцієнт, що враховує КПО за рахунок відбиття від поверхонь приміщення і підстилаючого шару, для даного приміщення становить r1=1.3 .

Для вікон з подвійними рамами коефіцієнт світлопропускання τ1=0,8 . Оскільки палітурка вікна подвійний дерев'яний, то τ2=0,6. При бічному освітленні τ3=1. В якості сонцезахисних пристроїв використовуються регульовані внутрішні штори, тому τ4=0,9. Таким чином, отримуємо

;

;

Таким чином, коефіцієнт природної освітленості е=0,62% задовольняє нормі. Природне освітлення суттєво залежить від погодних умов, отже, необхідно передбачити штучне освітлення в похмуру погоду. Штучне освітлення необхідно ще й тому, що в приміщенні ведуться роботи не тільки в світлий час доби, але і в темний.

Як джерело світла виберемо люмінесцентні лампи, оскільки вони володіють великою економічністю і світловіддачою, ніж лампи розжарювання. У зв'язку з цим найбільш доцільно вибрати систему загального освітлення.

Згідно СНИП II -4-79 виконувані зорові роботи відносяться до IV розряду зорових робіт (здатність розрізняти деталі від 0.5 до 1 мм). Підрозряд зорових робіт - В, так як фон середній, а контраст об'єкта з фоном теж середній.

Штучне освітлення нормується за СНИП II -4-79, згідно з якими в складальних цехах освітленість робочого місця повинна становити 300 лк. Для створення такого рівня освітленості використовуються світильники ЛВ001, що містять по чотири лампи ЛБ потужністю по 40 Вт, світловіддачою 70 лм/Вт і розмістимо їх на стелі.

Необхідна кількість світильників

                                                         (4.6)

 де N - кількість світильників, шт.;

ЕН - нормована мінімальна освітленість, лк;

КЗ = 1.3 - коефіцієнт запасу, що залежить від вмісту пилу в приміщенні, раз (приймається в межах від 1.3. До 2.0 залежно від вмісту пилу у виробничих приміщеннях з урахуванням регулярного очищення світильників і виду джерела світла);

S - площа освітлюваного приміщення, м 2;

z - коефіцієнт нерівномірності освітлення;

n = 4 - число ламп у світильнику, шт;

F = 2800 лм - світловий потік однієї лампи;

η - коефіцієнт використання світлового потоку, що залежить від індексу приміщення.

Розрахуємо індекс приміщення за наступним виразом

                                         (4.7)

де i - індекс приміщення;

А - довжина приміщення, м;

В - ширина приміщення, м;

h - розрахункова висота, м.

Визначимо розрахункову висоту як

                                        (4.8)

де Н - висота приміщення, м;

h 2 - висота звису, м;

h 1 - висота робочої поверхні, м.

 Висота приміщення H = 5 м, висота робочої поверхні h1= 0.8 м, висота звису для даного типу світильників h2= 0 м. Підставляючи дані величини в формулу (5.8), отримуємо

,м

При довжині А = 20 м і ширині В = 5 м індекс приміщення, відповідно до виразу (5.7), становитиме:



Приймаючи коефіцієнт відбиття від стін і стелі рівними 50% і 30% відповідно і з урахуванням отриманого індексу приміщення і типу світильника, величина використання світлового потоку складає η = 49%. При нормі освітленості 300 лк, площі приміщення SП=100м2, коефіцієнт нерівномірності освітлення z = 1.1, коефіцієнт запасу КЗ= 1.3, світловий потік однієї лампи 2800 лк, кількість світильників, згідно з формулою (5.6), становитиме:

 , шт

Таким чином число світильників дорівнює N = 8. Розташуємо світильники в два ряди вздовж довгих стін по чотири світильника. Розрахуємо відстань між світильниками:

 ;

Розрахуємо відстань від крайнього ряду світильників до стін:



 Пожежі у виробничих приміщеннях, де встановлено обладнання, становлять особливу небезпеку, тому що пов'язані як з матеріальними втратами, так і з відмовою обладнання та обчислювальної техніки, що в свою чергу тягне за собою порушення ходу технологічного процесу.

У виробничому приміщенні присутні наступні горючі речовини:

* дерево (столи, двері);
* пластмаса (компоненти ЕРЕ, корпусу);
* скловолокна (плати ЕОТ);
* полімери (ізоляція, покриття підлог) і т.д.

 Пожежовибухонебезпека застосовуваних матеріалів наведена в таблиці 4.1.

Внаслідок наявності пожежонебезпечних матеріалів, відповідно до виробниче приміщення належить до категорії В.

Можливі такі причини виникнення пожежі:

* іскри і дуги коротких замикань;
* іскри при розмиканні і замиканні ланцюгів;
* перегріви при тривалому навантаженні;
* нагрів індукційними струмами;
* нагрівання від діелектричних втрат;
* розряди статичної електрики.

 Таблиця 4.1 - Пожежовибухонебезпека матеріалів

|  |  |  |
| --- | --- | --- |
| Матеріал | Показник небезпеки | Засоби гасіння |
| Поліаміди(Матеріал корпусу мікросхем) | Горюча речовинаtвоспл 315 ° Сtсамовоспл 420 ° Сенергія запалювання 200мДж | гасити розпиленою водою зі змочувачами, піною, порошком ПФ (фосфорно-аммонійним) |
| Лак електроізоляційний (покриття друкованих плат) | Горюча речовина,tвоспл 141 ° Сtсамовоспл 379 ° С | гасити розпиленою водою зі змочувачами, піною, порошком ПФ (фосфорно-аммонійним) |
| Полістирол ударостійкий (корпуси ЕРЕ) | Горюча речовина,tвоспл 343 ° Сtсамовоспл 486 ° С | розпорошена вода зі змочувачами |
| Склотекстоліт (друковані плати) | Важкозаймистий матеріал, схильний до теплового самозаймання tсамонагр 120 ° Сtвоспл 285 ° Сtсамовоспл 480 ° С | розпорошена вода зі змочувачами |
| Олово(Пайка ЕРЕ) | Горюча речовина,tвоспл 430 ° Сенергія запалювання 80 мДж | Оберігати від джерел нагріву з температурою вище 80 0С, гасити розпиленою водою зі змочувачем |

Вивчення показало, що неможливо виключити із застосування горючі і пожаровибухонебезпечні матеріали, тому проектується зменшувати ймовірність утворення горючих середовищ в робочому приміщенні, що досягається застосуванням таких заходів пожежної безпеки:

* виключення можливості появи іскрового розряду в займистою середовищі з енергією, рівною і вище мінімальної енергії запалювання;
* вживання не іскристого інструменту при роботі з легкозаймистими рідинами;
* застосування машин, механізмів, устаткування, пристроїв, при експлуатації яких не утворюються джерела запалювання;
* виконанням чинних будівельних норм, правил і стандартів.

Протипожежний захист досягається застосуванням автоматичних установок пожежної сигналізації та застосуванням засобів пожежогасіння.

Приміщення обладнується відповідно до "Типових правил пожежної безпеки для промислових підприємств" автоматичною пожежною сигналізацією з димовими сповіщувачами фотоелектричного типу ІДФ-М, призначених для виявлення початкової стадії пожежі по появі диму в місці його розташування та видачі тривожного сигналу на станцію пожежної сигналізації. Причому відповідно до розрахункових даних і параметрів сповіщувача ІДФ-М, на площу 100м2необхідно чотири сповіщувачі.

 Висновки.

 У даній роботі розглянуті тенденції розвитку GSM-систем охорони, основні технічні характеристики стільникових мереж стосовно системам охорони. Зроблені технічно обґрунтовані висновки про те, що GSM-системи в даний час є найбільш оптимальними серед інших радіо канальних систем для використання, а також що вкрай ефективним є використання GSM-каналу в поєднанні з іншими каналами передачі повідомлень (що на даний момент реалізується повсюдно). GSM-системи мають ряд незаперечних переваг:

- можливість використання сервісів оператора стільникового зв'язку для надання послуг охорони;

- простоту і зручність застосування;

- доступність стільникового зв'язку переважній більшості громадян;

- відсутність необхідності купувати ретранслятори для роботи системи.

Проведено аналіз основних функцій GSM-мереж, їх використання в системах охорони. Проведено дослідження швидкості передачі даних і пропускної здатності GSM каналу. Розглянуті механізми побудови GSM-каналу, його основні технічні характеристики. Сформульовані рекомендації щодо поліпшення технічних характеристик систем безпеки, що використовують GSM-канали.

 Література

1. Крухмалёв В.В., Гордиенко Н.В., Моченов А.Д. и др. Основы построения телекоммуникационных систем и сетей: учебник для вузов. - М.: Горячая линия - Телеком, 2004. - 510 с.

2. Громаков Ю.А. Стандарты и системы подвижной радиосвязи. - М.: Эко-Трендз, 2008. – 144с.

3. Берлин А.Н. Сотовые системы связи / Издательство: «Интернет-университет информационных технологий - ИНТУИТ.ру », БИНОМ. Лаборатория знаний , 2009. - 362 с.

4. Теодорович Н.Н. Системы безопасности в комплексном интеллектуальном здании // Промышленные АСУ и контроллеры. 2010. № 6. С. 54-55.

5. Анин, Б.Ю. Защита компьютерной информации / Б.Ю. Анин.— СПб.: BHV — Санкт-Петербург, 2000.

6. Карташевский, В.Г. Сети подвижной связи / В.Г. Карташевский, С.Н. Семенов, Т.В. Фирстова.— М.: Эко-Трендз, 2001.

7. Системы мобильной связи: учебное пособие для вузов / В.П. Ипатов, В.К. Орлов, И.М. Самойлов, В.Н. Смирнов; под ред. В.П. Ипатова.— М.: Горячая линия — Телеком, 2003.— 272 с., ил.

8. Кирилов, В.И. Многоканальные системы передачи: учебник / В.И. Кирилов.— 2-е изд.— М.: Новое знание, 2003.— 751 с.: ил.

9. Антенно-фидерные устройства и распространение радиоволн: учебник для вузов / Г.А. Ерохин, О.В. Чернышов, Н.Д. Козырев, В.Г. Кочержевский; под. ред. Г.А. Ерохина.— 2-е изд., испр.— М.: Горячая линия — Телеком, 2004.— 491 с.: ил.

10. Ксенофонтов, С.Н. Направляющие системы электросвязи: учебное пособие для вузов / С.Н. Ксенофонтов, Э.Л. Портнов.— М.: Горячая линия — Телеком, 2004, — 268 с.: ил.

11. Тепляков, И.М. Основы построения телекоммуникационных систем и сетей: учебное пособие / И.М. Тепляков.— М.: Радио и связь, 2004.— 328 с.

12. Адрианов, В.И. Сотовые, пейджинговые и спутниковые средства связи / В.И. Адрианов, А.В. Соколов.— СПб.: BHV — Санкт-Петербург; Арлит, 2001.

13. Урядников Ф.Ю. Сверхширокополосная связь. Теория и применение / Ф.Ю. Урядников, С.С. Аджемов.— М.: СОЛОН-Пресс, 2005.— 368 с.— (Серия «Библиотека студента»)

14. Адрианов, В.И. Средства мобильной связи / В.И. Адрианов, А.В. Соколов.— СПб.: BHV — Санкт-Петербург, 1998.

15. Ратынский, М.В. Основы сотовой связи / М.В. Ратынский.— М.: Радио и связь, 1998.

16. Системы цифровой радиосвязи: базовые методы и характеристики: Учеб. пособие Волков Л.Н., Немировский М.С., Шинаков Ю.С. (2009 г.)

17. Красс М.С. Математика для экономических специальностей: Учебник. – 4 – е изд., испр. – М.: Дело, 2003. – 704 с.

18. Системы и сети передачи информации: Учеб. пособие для вузов / М.В. Гаранин, В.И. Журавлев, С.В. Кунегин.

19. Охрана труда в электроустановках: Учебник для вузов / Под ред. Б.А. Князевского. – М.: Энергоатомиздат, 1983. – 336 с.

20. Ткачук К.Н., Сабарно Р.В. Охрана труда и окружающей среды в радиоэлектронной промышленности. – К.: Вища школа, 1988.

21. Пожаровзрывоопасность веществ и материалов и средства их тушения. Справочник / Под ред. Баратова А.Н., в 2-х томах. – М.: Химия, 1990.

22. Добровольский А.А., Переслыцких Х.Х. Пожарная техника. Справочник. – К.: Техника, 1981.