GSM information security system improvement

Dmytro Knyazyev

Information Security Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12,
E-mail: shamanlviv@gmail.com

In this report, we have examined trends in GSM-protection systems, the main technical characteristics of mobile networks in relation to the systems of protection. Technically valid conclusions have been made about the fact that GSM-systems are currently the most suitable radio channel systems, among other systems to use. With the development of communication systems using mobile networks there will be more benefits and security GSM-systems will come to a new level of quality, reliability and availability to users. I concluded that it is extremely effective to use GSM-channel in combination with other types of channels. GSM-systems have a number of advantages:

- the use of mobile operator services for the provision of security services;
- simplicity and ease of use;
- availability of mobile communications for the majority of citizens;
- no need to purchase repeaters for the system.

For now, the use of third generation networks already opens up many additional opportunities to significantly improve the functionality of the GSM-protection systems. We have analyzed the main features of GSM-networks, their use in security systems. Also the speed and bandwidth of GSM channels were analyzed.

Calculation of the average base station coverage area of GSM-900 and calculation of the load per cell have been made, on the basis of which we concluded about the level of reliability of such system.

In this work we have considered the construction mechanism of GSM-channel, its basic characteristics. Until now, one of the main drawbacks of GSM-channel is its poor antijamming immunity (together with the availability of devices to jam the signal), which makes its single application inefficient.

Based on the report several recommendations have been made to improve the performance of security systems that use GSM-channels. Based on these we have come to logical conclusions about possible ways to develop wireless security systems.

Вдосконалення систем захисту інформації, що використовують канали GSM

Дмитро Князєв

Кафедра захисту інформації, Національний університет “Львівська політехніка”, УКРАЇНА, м.Львів, вул.С.Бандери, 12,
E-mail: shamanlviv@gmail.com

У роботі здійснюється аналіз тенденцій розвитку GSM-систем охорони, основних технічних характеристик стільникових мереж щодо систем охорони. Були наведені технічно обгрунтовані висновки про те, що GSM-системи в даний час є найефективнішими для використання серед інших радіоканальних систем.

Ключові слова – система безпеки, радіоканал, GSM-канал, завадозахищеність, охоронна сигналізація.

І. Вступ

З розвитком систем передавання інформації по стільникових мережах переваг у радіоканальних систем стає все більше, і охоронні GSM-комплекси виходять на новий рівень якості, надійності та доступності для користувачів. Експерти вважають, що ефективним є використання GSM-каналу в поєднанні з іншими каналами передавання повідомлень (що на даний момент широко реалізується). GSM-системи мають декілька вагомих переваг:

- можливість використання сервісів операторів стільникового зв'язку для надання послуг охорони;
- простота і зручність застосування;
- доступність стільникового зв'язку переважній більшості громадян;
- відсутність необхідності купувати ретранслятори для роботи системи. [1]

Вже зараз використання мереж третього покоління відкриває безліч додаткових можливостей, значно підвищуючи функціональність GSM-систем охорони.

На основі проведених досліджень і розрахунків сформулюємо ряд рекомендацій щодо покращення технічних характеристик систем безпеки, що використовують GSM-канали, наведемо можливі шляхи розвитку безпровідних систем охорони.

На цей час ринок послуг та обладнання охоронно-пожежної сигналізації стрімко зростає. Проте, до недавнього часу основним недоліком систем охоронної та пожежної сигналізації (ОПС) було використання провідних телефонних ліній. До основних недоліків даних систем віднесемо нестійку роботу міських телефонних ліній, низьку фізичну захищеність, відсутність можливості охорони нетелефонізованих об’єктів (дачі, котеджі і т. д.). Тому, як надійна альтернатива «провідним охоронним системам» з’явився новий напрям - «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 (у межах зони дії радіоканальної мережі).
- універсальність – з простих елементів можна побудувати якзавгодно складну систему: висока швидкість монтажу і запуску в експлуатацію, можливість оперативної зміни конфігурації, мобільність охоронного пульта, можливість співіснування кількох пультів. Немає принципових обмежень для під'єднання до існуючої системи охорони .

Спочатку безпровідні системи не отримали широкого поширення через низьку надійність (провідний зв'язок в цьому плані ще років п'ять назад був надійнішим). Але на цей час з'явився широкий спектр різних додаткових пристроїв, активно використовуються нові покоління безпровідних систем зв'язку.

Широке 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 безпровідні охоронні системи на базі GSM отримали широке розповсюдження завдяки їх відносно невисокій вартості і простоті встановлення і експлуатації. Мережа стандарту GSM-900/1800 забезпечує кращу якість зв'язку та вже розгорнута у більшості міст України та країн СНД.

Системи, що використовують GSM-зв'язок, дають змогу здійснити охорону будь-яких об'єктів, у тому числі і нетелефонізованих. Використання GSM позбавляє від необхідності розгортати свою мережу ретрансляторів – використовуються ретранслятори GSM-операторів. Внаслідок цього можна брати під охорону об'єкт скрізь, де впевнено працює мережа GSM-оператора.

І, звичайно, дуже перспективним видається використання нових протоколів і мереж 3G, які спеціально призначені для корпоративних клієнтів – віртуальні корпоративні мережі передавання даних (VPN) з реалізацією імітостійкості і захисту інформації.

Проте, істотним недоліком таких систем є низька завадозахищеність. Відомо, що GSM-канал легко подавити, «GSM глушилки» перебувають сьогодні у вільному продажу, та й робота мережі GSM не завжди відрізняється високою стабільністю і може відмовити в самий відповідальний момент. Хоча останні розроблення дозволяють повністю контролювати GSM-канал, оперативно змінювати частоти, що помітно підвищує завадозахищеність.

Оптимально використовувати GSM-канал як дублюючий або додатковий до провідних або інших радіоканальних систем. Суттєвою перевагою GSM-систем є можливість самого клієнта контролювати стан об'єкту і керувати його охороною.

II. Завадостійкість і завадозахищеність GSM каналів

Перешкоди в радіоканалі створюються як за рахунок спотворень сигналу при його поширенні, так і в результаті впливу зовнішніх джерел. Перший тип спотворень можна порівняно легко усунути, в той же час з перешкодами від зовнішніх джерел борються за допомогою розширення спектру передаваного сигналу. Теоретично, збільшення бази сигналу (добуток 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 до переривання передачі даних й 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 РЕС, що використовують вузькосмугові сигнали, застосовують багаторазове дублювання фрагментів переданих повідомлень в частотній або часовій 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 повільна псевдовипадкова чи програмна перебудова радіочастот (ППРЧ). Використання ППРЧ спільно з завадостійким кодуванням і перечередуванням дозволяє в умовах вузькосмугових завад в каналах з завмираннями підвищити завадостійкість на прийомі на 9-11дБ, в той час, як без ППРЧ ця цифра коливається в межах 4-6дБ. [1]

Перешкодостійкість, на думку цілого ряду фахівців в області радіоканальних пожежних і охоронних систем, визначається :

- Кількістю частотних діапазонів, в яких може працювати радіосистема;
- Кількістю частотних каналів у кожному діапазоні;
- Можливістю автоматичного вибору резервних каналів;
- Наявністю автоматичного регулювання потужності випромінювання. [2]

Відповідно до європейської класифікації [1] існує три класи пожежних і охоронних провідних і радіоканальних 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'ятники).

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. 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 дії організованих перешкод називається завадозахищеністю.

Завадозахищеність поділяється на два класи:

1) просторова завадозахищеність (за рахунок низького рівня бічних пелюсток прийомної антени, по яких діє завада, формування «нулів» діаграми спрямованості приймальної антени в напрямі на джерело перешкод);

2) сигнальна завадозахищеність за рахунок широкосмугових методів модуляції.

Принцип придушення заснований на постановці вузькосмугової 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. Широкосмугова глушилка. Постійно випромінює потужний шум на всіх робочих частотах GSM. Тим самим GSM-модуль перестає бачити як супутники GPS, що передають поточні координати автомобіля, так і базову станцію оператора GSM.

2. Перебираюча частоти - цей тип глушилок працює так як перший тип, відмінність у тому, що шумоподібна перешкода ставиться послідовно по всіх частотах каналу GSM, не дозволяючи GSM-модулю 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 сповіщення. Але це малоймовірно, адже відправити SMS або голосове повідомлення навряд вийде, тому що передавач вже заглушений.

- Визначення факту глушіння ззовні. Для цього організується постійна перевірка зв'язку між GSM-модулем і спеціально виділеним сервером - контроль каналу. Таким чином, на стороні сервера можна гарантовано визначити втрату зв'язку. У разі втрати GSM-сигналу, сервер оповіщає 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;
- Застосування виносних антен. [2]

III. Розробка рекомендацій щодо покращення технічних характеристик систем безпеки, що використовують канали GSM

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 ускладнено прокладання 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 та 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 та включення інших пристроїв.

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

Третя умова – особливу увагу необхідно приділити наявності і 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 вольт.

Четверта умова – 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 умова – добре, щоб система могла в одному повідомленні повністю описувати стан всієї системи: тривоги з вказівкою зони, стану системи, описувати, які реле включені, скільки залишилося заряду в батареї, який стан телефонної лінії (якщо вона є). Існують й 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 блокувати стільникову мережу в окрузі за допомогою банальної стільникової «глушилки», тому важливо, щоб у відповідь, скажімо, на вторгнення, система не тупо перебирала номери для повідомлення настільки «доброї» новини, а відразу відкривала клітки з собаками-охоронцями, запалювала світло, включала сирену або пускала сльозогінний газ.

Шоста умова - 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 користувачам і пультам 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 з вказівкою 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 граничної віддаленості від найближчої базової станції (БС)
- Робота всередині зони покриття, але в місцях радіотіні (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 у вельми 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 у період великих свят. Рішенням проблеми є встановлення об'єктового приладу з sim-картами двох різних стільникових операторів зв'язку. Оптимальним для GSM-сигналізацій є комбінування різних функцій (SMS, Voice). Також ефективним є використання GSM як дублюючий або додатковий канал проводових і інших радіоканальних систем передачі повідомлення.

З точки зору пропускної здатності каналу виправдане використання технології EDGE. Правда, ця технологія (як і 3G) не отримала ще повсюдного поширення.

Висновок

У даній роботі описані найвагоміші недоліки систем безпеки, що використовують GSM-канали, та сформульований ряд рекомендацій щодо покращення їх технічних характеристик.

Література

[1] Основы построения телекоммуникационных систем и сетей: учебник для вузов / В.В. Крухмалёв, Н.В. Гордиенко, А.Д. Моченов и др.; под. ред. В.Н. Гордиенко и В.В. Крухмалёва.— М.: Горячая линия — Телеком, 2004.— 510 с.

[2] 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.